DATA PROTECTION LAWS OF THE WORLD

Full Handbook

DLA PIPER

TABLE OF CONTENTS

ABSTRACT

More than ever it is crucial that organizations manage and safeguard personal information and address their risks and legal responsibilities in relation to processing personal data, to address the growing thicket of applicable data protection legislation.

A well-constructed and comprehensive compliance program can solve these competing interests and is an important risk management tool.

This handbook sets out an overview of the key privacy and data protection laws and regulations across nearly 100 different jurisdictions and offers a primer to businesses as they consider this complex and increasingly important area of compliance.

DLA Piper's global data protection and privacy team has the deep experience and international reach to help global businesses develop and implement practical compliance solutions to the myriad data protection laws that apply to global businesses.

INTRODUCTION

Welcome to DLA Piper's Data Protection Laws of the World Handbook. We launched the first edition of the handbook in 2012, and following such a positive response have been updating it annually ever since.

We continue to witness a period of unprecedented activity in the development of data protection regulation around the world which will have a profound impact on the way in which global businesses are required to approach the collection and management of personal information.

These changes are being driven largely by cultural and trade considerations and by a struggle to keep pace with emerging technology and online business methods.

Should you require further guidance, please do not hesitate to contact us at dataprivacy@dlapiper.com.

DATA PRIVACY SCOREBOX

You may also be interested in our Data Privacy Scorebox, a tool to help you assess your data protection strategy. It requires completing a survey covering 12 areas of data privacy, such as storage of data, use of data, and customers' rights. Once completed, a report summarizing your organization's alignment with key global principles of data protection is produced. The report includes a visual summary of the strengths and weaknesses of your data protection strategy, a practical action point checklist, as well as peer benchmarking data.

To access the Scorebox, please visit www.dlapiper.com/dataprotection.

CYBERTRAK

We are pleased to introduce CyberTrak, an innovative online cybersecurity tool featuring information on cybersecurity-related mandates in 23 key markets around the world. CyberTrak is the inaugural product of Blue Edge Lab℠.

CyberTrak provides multinational companies instant online access to critical information about cybersecurity-related laws, regulations and generally accepted standards in 23 key markets in the Americas, Asia-Pacific, Europe and the Middle East and in four highly regulated sectors in the US. It also provides brief summaries of requirements, as well as an assessment on enforcement risk and the degree of activity triggering the requirement.

Cybersecurity laws and regulations are evolving rapidly around the world. Companies battling ever more sophisticated cyberattacks face mounting compliance costs and higher risks if they do not keep up with new requirements in all markets where they operate.

CyberTrak is designed to help GCs, CIOs, CISOs, risk officers and legal, technology, IT and procurement departments of multinational companies make better, faster risk management decisions and reduce the costs associated with keeping up with these changing regulatory requirements.

CyberTrak content will be regularly updated three times per year by a global group of more than 50 carefully selected contributors in key jurisdictions (many of them contributors to Data Protection Laws of the World), along with interim updates when major changes occur.

Understanding cybersecurity mandates on a global scale is critical to any multinational company that collects and retains customer data, trade secrets, and other confidential data or operates in a critical infrastructure sector, such as energy, financial services, healthcare and defense/government contractors.

Company-wide CyberTrak access is offered on an annual subscription basis. To register for a free trial or to learn more about CyberTrak, please visit www.BlueEdgeLab.com.

**Blue Edge Lab, LLC is a wholly owned subsidiary of DLA Piper LLP (US). Blue Edge Lab is not a law firm and does not provide legal services.*

GDPR SITE

We are proud to present a dedicated site offering DLA Piper's insight into the General Data Protection Regulation, the once-in-a-generation change in EU data protection laws.

DATA PROTECTION BLOG

If you find this Handbook useful, you may also be interested in DLA Piper's Data Protection, Privacy and Security group's Privacy Matters Blog a blog featuring regular data protection, privacy and security legal updates to help you remain aware of the most important legal and regulatory developments.

We have over 130 experienced privacy and security lawyers across the globe who are close to the regulations in each of their respective jurisdictions and who regularly post summary articles on their local issues.

To access the blog, please visit http://blogs.dlapiper.com/privacymatters/.

To ensure you receive an automatic email when a new article is posted, please enter your details in the 'subscribe' section found on the blog's righthand sidebar.

DISCLAIMER

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

I. INTRODUCTION

EU data protection legislation is facing huge changes. Data protection laws are built on fundamental rights enshrined in the Charter of Fundamental Rights of the European Union which are the core building blocks of the EU's legal regime. Privacy issues arising from an exponential growth in consumer and mobile technologies, an increasingly connected planet and mass cross- border data flows have pushed the EU to entirely rethink its data protection legislation to ensure that these fundamental rights are fully protected in today's digital economy.

In 2012, the European Commission published a draft regulation (the General Data Protection Regulation, 'GDPR'). Just over four years later, the final text of GDPR was published in the Official Journal of the European Union on April 27, 2016. Regulation 2016/679 heralds some of the most stringent data protection laws in the world and has been in force since May 25, 2018.

The previous EU Data Protection Directive (95/46/EC) was adopted in 1995. It was implemented differently by EU Member States into their respective national jurisdictions, resulting in the fragmentation of national data protection laws within the EU. As it is a Regulation, GDPR came into effect immediately on May 25, 2018 without any need for additional domestic legislation in EU Member States. However, with more than 30 areas where Member States are permitted to legislate (differently) in their domestic laws there will continue to be significant variation in both substantive and procedural data protection laws among the EU's different Member States.

With fines of up to 4% of total worldwide annual turnover for failing to comply with the requirements of GDPR, organizations have had a great deal to do to comply with the new regime.

II. CURRENT SITUATION

After almost four years of often fractious negotiations, GDPR was published in the Official Journal of the European Union as Regulation 2016/679 on April 27, 2016.

There was a two-year transition period to allow organizations and governments to adjust to the new requirements and procedures. Following the end of this transitional period, the Regulation became directly applicable throughout the EU from May 25, 2018, without requiring implementation by the EU Member States through national law.

The goal of European legislators was to harmonize the previous legal framework, which was fragmented across Member States. A 'Regulation' (unlike a Directive) is directly applicable and has consistent effect in all Member States, and GDPR was intended to increase legal certainty, reduce the administrative burden and cost of compliance for organizations that are active in multiple EU Member States, and enhance consumer confidence in the single digital marketplace. However, in order to reach political agreement on the final text there are more than 30 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws. There continues to be room for different interpretation and enforcement practices among the Member States. There is therefore likely to continue to be significant differences in both substantive and procedural data protection laws and enforcement practice among EU Member States with GDPR in force.

We have summarized the key changes introduced by the GDPR in the following sections.

Key changes to the previous data protection framework include:

A. WIDER TERRITORIAL SCOPE

Where organizations are established within the EU

GDPR applies to processing of personal data "in the context of the activities of an establishment" (Article 3(1)) of any organization within the EU. For these purposes "establishment" implies the "effective and real exercise of activity through stable arrangements" (Recital 22) and "the legal form of such arrangements…is not the determining factor" (Recital 22), so there is a wide spectrum of what might be caught from fully functioning subsidiary undertakings on the one hand, to potentially a single individual sales representative depending on the circumstances.

Europe's highest court, the Court of Justice of the European Union (the CJEU) has been developing jurisprudence on this concept,

recently finding (*Google Spain SL, Google Inc. v AEPD*, *Mario Costeja Gonzalez* (C-131/12)) that Google Inc. with EU-based sales and advertising operations (in that particular case, a Spanish subsidiary) was established within the EU. More recently, the same court concluded (*Weltimmo v NAIH* (C-230/14)) that a Slovakian property website was also established in Hungary and therefore subject to Hungarian data protection laws.

Where organizations are not established within the EU

Even if an organization is able to prove that it is not established within the EU, it will still be caught by GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "to the offering of goods or services" (Art 3(2)(a)) (no payment is required) to such data subjects in the EU or "the monitoring of their behavior" (Art 3(2)(b)) as far as their behavior takes place within the EU. Internet use profiling (Recital 24) is expressly referred to as an example of monitoring.

Practical implications

1. Compared to the previous Directive, GDPR captures many more overseas organizations. US tech should particularly take note as the provisions of GDPR have clearly been designed to capture them.

2. Overseas organizations not established within the EU who are nevertheless caught by one or both of the offering goods or services or monitoring tests must designate a representative within the EU (Article 27).

B. TOUGHER SANCTIONS

Revenue-based fines

GDPR joins anti-bribery and anti-trust laws as having some of the very highest sanctions for non-compliance including revenue-based fines of up to 4% of annual worldwide turnover.

To compound the risk for multinational businesses, fines are imposed by reference to the revenues of an undertaking rather than the revenues of the relevant controller or processor. Recital 150 of GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully the Treaty doesn't define the term either and the extensive case-law is not entirely straightforward with decisions often turning on the specific facts of each case. However, in many cases group companies have been regarded as part of the same undertaking. This is bad news for multinational businesses as it means that in many cases group revenues will be taken into account when calculating fines, even where some of those group companies have nothing to do with the processing of data to which the fine relates provided they are deemed to be part of the same undertaking. The assessment will turn on the facts of each case.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to 20,000,000 Euros or in the case of an undertaking up to 4% of total worldwide turnover of the preceding year, whichever is higher apply to breach of:

- the basic principles for processing including conditions for consent
- data subjects' rights
- international transfer restrictions
- any obligations imposed by Member State law for special cases such as processing employee data
- certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to 10,000,000 Euros or in the case of an undertaking up to 2% of total worldwide turnover of the preceding year, whichever is the higher apply to breach of:

- obligations of controllers and processors, including security and data breach notification obligations
- obligations of certification bodies
- obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Broad investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

GDPR makes it considerably easier for individuals to bring private claims against data controllers and processors. In particular:

- any person who has suffered "material or non-material damage" as a result of a breach of GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress and hurt feelings even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80). Although this falls someway short of a US style class action right, it certainly increases the risk of group privacy claims against consumer businesses. Employee group actions are also more likely under GDPR.

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Practical implications

1. The scale of fines and risk of follow-on private claims under GDPR means that actual compliance is a must. GDPR is not a legal and compliance challenge – it is much broader than that, requiring organizations to completely transform the way that they collect, process, securely store, share and securely wipe personal data. Engagement of senior management and forming the right team is key to successful GDPR readiness.

2. Organizations caught by GDPR need to map current data collection and use, carry out a gap analysis of their current compliance against GDPR and then create and implement a remediation plan, prioritizing high risk areas.

3. GDPR requires suppliers and customers to review supply chains and current contracts. Contracts will need to be renegotiated to ensure GDPR compliance and commercial terms will inevitably have to be revisited in many cases given the increased costs of compliance and higher risks of non-compliance.

4. The very broad concept of 'undertaking' is likely to put group revenues at risk when fines are calculated, whether or not all group companies are caught by GDPR or were responsible for the infringement of its requirements. Multinationals even with quite limited operations caught by GDPR will therefore need to carefully consider their exposure and ensure compliance.

5. Insurance arrangements need to be reviewed and cyber and data protection exposure added to existing policies or purchased as stand-alone policies where possible. The terms of policies require careful review as there is wide variation among wordings and many policies may not be suitable for the types of losses which are likely to occur under GDPR.

C. MORE DATA CAUGHT

Personal data is defined as "any information relating to an identified or identifiable natural person." (Article 4) A low bar is set for "identifiable" – if anyone can identify a natural person using "all means reasonably likely to be used" (Recital 26) the information is

personal data, so data may be personal data even if the organization holding the data cannot itself identify a natural person. A name is not necessary either – any identifier will do such as an identification number, location data, an online identifier or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30 with IP addresses, cookies and RFID tags all listed as examples.

Although the definition and recitals are broader than the equivalent definitions in the current Directive, for the most part they are simply codifying current guidance and case law on the meaning of 'personal data'.

GDPR also includes a broader definition of "special categories" (Article 9) of personal data which are more commonly known as sensitive personal data. The concept has been expanded to expressly include the processing of genetic data and biometric data. The processing of these data are subject to a much more restrictive regime.

A new concept of 'pseudonymisation' (Article 4) is defined as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Organizations which implement pseudonymization techniques enjoy various benefits under GDPR.

Practical implications

1. If in any doubt, it is prudent to work on the assumption that data is personal data given the extremely wide definition of personal data in GDPR.

2. GDPR imposes such a high bar for compliance, with sanctions to match, that often the most effective approach to minimize exposure is not to process personal data in the first place and to securely wipe legacy personal data or render it fully anonymous, reducing the amount of data subject to the requirements of GDPR.

3. Where a degree of identification is required for a specific purpose, the next best option is only to collect and use pseudonymous data. Although this falls within the regulated perimeter, it enjoys a number of benefits for organizations in particular that in the event of a data breach it is much less likely that pseudonymous data will cause harm to the affected individuals, thereby also reducing the risk of sanctions and claims for the relevant organization.

4. Organizations should only use identifiable personal data as a last resort where anonymous or pseudonymous data is not sufficient for the specific purpose.

D. SUPPLIERS (PROCESSORS) CAUGHT TOO

GDPR directly regulates data processors for the first time. The current Directive generally regulates controllers (i.e., those responsible for determining the purposes and means of the processing of personal data) rather than 'data processors' - organizations who may be engaged by a controller to process personal data on their behalf (e.g., as an agent or supplier).

Under GDPR, processors are required to comply with a number of specific obligations, including to maintain adequate documentation (Article 30), implement appropriate security standards (Article 32), carry out routine data protection impact assessments (Article 32), appoint a data protection officer (Article 37), comply with rules on international data transfers (Chapter V) and cooperate with national supervisory authorities (Article 31). These are in addition to the requirement for controllers to ensure that when appointing a processor, a written data processing agreement is put in place meeting the requirements of GDPR (Article 28). Again, these requirements have been enhanced and gold-plated compared to the equivalent requirements in the Directive.

Processors are directly liable to sanctions (Article 83) if they fail to meet these criteria and may also face private claims by individuals for compensation (Article 79).

Practical implications

1. GDPR completely changes the risk profile for suppliers processing personal data on behalf of their customers. Suppliers now

face the threat of revenue-based fines and private claims by individuals for failing to comply with GDPR. Telling an investigating supervisory authority that you are just a processor won't work; they can fine you too. Suppliers need to take responsibility for compliance and assess their own compliance with GDPR. In many cases, this requires the review and overhaul of current contracting arrangements to ensure better compliance. The increased compliance burden and risk requires a careful review of business cases.

2. Suppliers need to decide for each type of processing undertaken whether they are acting solely as a processor or if their processing crosses the line and renders them a data controller or joint controller, attracting the full burden of GDPR.

3. Customers (as controllers) face similar challenges. Supply chains need to be reviewed and assessed to determine current compliance with GDPR. Privacy impact assessments need to be carried out. Supervisory authorities may need to be consulted. In many cases contracts are likely to need to be overhauled to meet the new requirements of GDPR. These negotiations will not be straightforward given the increased risk and compliance burden for suppliers. They will also be time consuming and it would be sensible to start the renegotiation exercise sooner rather than later, particularly as suppliers are likely to take a more inflexible view over time as standard positions are developed.

4. There are opportunities for suppliers to offer GDPR "compliance as a service" solutions, such as secure cloud solutions, though customers will need to review these carefully to ensure they dovetail to their own compliance strategy.

E. DATA PROTECTION PRINCIPLES

The core themes of the data protection principles in GDPR remain largely as they were in the Directive, though there has been a significant raising of the bar for lawful processing (see Higher Bar for Lawful Processing) and a new principle of accountability has been added.

Personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle")
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle")
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle")
- accurate and where necessary kept up-to-date (the "accuracy principle")
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle")
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle")

The controller is responsible for and must be able to demonstrate compliance with the above principles (the accountability principle).

Practical implications

1. Controllers need to assess and ensure compliance of data collection and use across their organizations with each of the above principles as any failure to do so attracts the maximum category of fines of up to 20 million Euros / 4% of worldwide annual turnovers. Data mapping, gap analysis and remediation action plans need to be undertaken and implemented.

2. The enhanced focus on accountability will require a great deal more papering of process flows, privacy controls and decisions made to allow controllers to be able to demonstrate compliance. See Accountability and Governance

F. HIGHER BAR FOR LAWFUL PROCESSING

The lawfulness, fairness and transparency principle among other things requires processing to fall within one or more of the permitted legal justifications for processing. Where special categories of personal data are concerned, additional much more restrictive legal justifications must also be met.

Although this structure is present in the Directive, the changes introduced by GDPR will make it much harder for organizations to

fall within the legal justifications for processing. Failure to comply with this principle is subject to the very highest fines of up to 20 million Euros or in the case of an undertaking up to 4% of annual worldwide turnover, whichever is the greater.

In particular:

- The bar for valid consents has been raised much higher under GDPR. Consents must be fully unbundled from other terms and conditions and will not be valid unless freely given, specific, informed and unambiguous (Articles 4(11) and 6(1)(a)). Consent also attracts additional baggage for controllers in the form of extra rights for data subjects (the right to be forgotten and the right to data portability) relative to some of the other legal justifications. Consent must be as easy to withdraw consent as it is to give – data subjects have the right to withdraw consent at any time – and unless the controller has another legal justification for processing any processing based on consent alone would need to cease once consent is withdrawn.
- To compound the challenge for controllers, in addition to a hardening of the requirements for valid consent, GDPR has also narrowed the legal justification allowing data controllers to process in their legitimate interests. This justification also appears in the Directive though the interpretation of the concept in the current regime has varied significantly among the different Member States with some such as the UK and Ireland taking a very broad view of the justification and others such as Germany taking a much more restrictive interpretation. GDPR has followed a more Germanic approach, narrowing the circumstances in which processing will be considered to be necessary for the purposes of the legitimate interests of the controller or a third party. In particular, the ground can no longer be relied upon by public authorities. Where it is relied upon, controllers will need to specify what the legitimate interests are in information notices and will need to consider and document why they consider that their legitimate interests are not overridden by the interests or fundamental rights and freedoms of the data subjects, in particular where children's data is concerned.

The good news is that the justification allowing processing necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject to enter into a contract is preserved in GDPR, though continues to be narrowly drafted. Processing which is not necessary to the performance of a contract will not be covered. The less good news for controllers relying on this justification is that it comes with additional burdens under GDPR, including the right to data portability and the right to be forgotten (unless the controller is able to rely on another justification).

Other justifications include where processing is necessary for compliance with a legal obligation; where processing is necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent; where processing is necessary for performance of a task carried out in the public interest in the exercise of official authority vested in the controller. These broadly mirror justifications in the previous Directive.

Processing for new purposes

It is often the case that organizations will want to process data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data was first collected. This is potentially in conflict with the core principle of purpose limitation and to ensure that the rights of data subjects are protected, GDPR sets out a series of considerations that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are a fresh consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Processing of special categories of personal data

As is the case in the Directive, GDPR sets a higher bar to justify the processing of special categories of personal data. These are defined to include "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation." (Article 9(1)) Processing of these data are prohibited unless one or more specified grounds are met which are broadly similar to the grounds set out in the Directive.

Processing of special categories of personal data is only permitted (Article 9(2)):

- with the explicit consent of the data subject
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- in limited circumstances by certain not-for-profit bodies
- where processing relates to the personal data which are manifestly made public by the data subject
- where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

The justifications and conditions for processing special categories of data is one area where Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Processing of personal data relating to criminal convictions and offenses

GDPR largely mirrors the requirements of the Directive in relation to criminal conviction and offences data. This data may only be processed under official authority or when authorized by Union or Member State law (Article 10) which means this is another area where legal requirements and practice is likely to diverge among the different Member States.

Practical Implications

1. Controllers need to ensure that they have one or more legal justifications to process personal data for each purpose. Practically this will require comprehensive data mapping to ensure that all personal data within the extended enterprise (i.e. including data processed by third parties as well as data within the organization) has a legal justification to be processed.

2. Consideration needs to be given as to which are the most appropriate justifications for different purposes and personal data, given that some justifications attract additional regulatory burdens.

3. The common practice of justifying processing with generic consents needs to cease with GDPR in force. Consent comes with many additional requirements under GDPR and as such is likely to be a justification of last resort where no other justifications are available.

4. Where controllers propose to process legacy data for new purposes, they need to be able to demonstrate compliance with the purpose limitation principle. To do that, controllers should document decisions made concerning new processing, taking into account the criteria set out in GDPR and bearing in mind that technical measures such as encryption or psuedonymisation of data will generally make it easier to prove that new purposes are compatible with the purposes for which personal data were originally collected.

G. TRANSFERS

International transfers and particularly those to the US have regularly made front page headline news over the last 12 months with the successful torpedoing of the EU/US Safe Harbor regime by Europe's highest court. Organizations will be relieved to hear that for the most part GDPR does not make any material changes to the previous rules for transfers of personal data cross-border, largely reflecting the regime under the Directive. That said, in contrast to the previous regime where sanctions for breaching transfer restrictions are limited, failure to comply with GDPR's transfer requirements attract the highest category of fines of up to 20 million Euros or in the case of undertakings up to 4% of annual worldwide turnover.

Transfers of personal data to third countries outside the EU are only permitted where the conditions laid down in GDPR are met (Article 44).

Transfers to third countries, territories or specified sectors or an international organization which the Commission has decided ensures an adequate level of protection do not require any specific authorization (Article 45(1)). The adequacy decisions made under the current Directive shall remain in force under GDPR until amended or repealed (Article 45(9)); so for the time being transfers to any of the following countries are permitted: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

The well-publicized gap for transfers from the EU to US following the ruling that Safe Harbor is invalid will, it is hoped, be filled with the new EU/US Privacy Shield.

Transfers are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards include among other things binding corporate rules which now enjoy their own Article 47 under GDPR and standard contractual clauses. Again, decisions on adequacy made under the Directive will generally be valid under GDPR until amended, replaced or repealed.

Two new mechanics are introduced by GDPR to justify international transfers (Article 46(2)(e) and (f)): controllers or processors may also rely on an approved code of conduct pursuant to Article 40 or an approved certification mechanism pursuant to Article 42 together in each case with binding and enforceable commitments in the third country to apply these safeguards including as regards data subjects' rights. GDPR also removes the need to notify and in some Member States seek prior approval of model clauses from supervisory authorities.

GDPR includes a list of derogations similar to those included in the Directive permitting transfers where:

(a) explicit informed consent has been obtained
(b) the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
(d) the transfer is necessary for important reasons of public interest
(e) the transfer is necessary for the establishment, exercise or defense of legal claims
(f) the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
(g) the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanic is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48)are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; otherwise transfer in response to such requests where there is no other legal basis for transfer will breach GDPR's restrictions.

Practical Implications

1. Given the continued focus of the media and regulators on international transfer and the increased sanctions to be introduced by GDPR, all controllers and processors need to carefully diligence current data flows to establish what types of data is being shared with which organizations in which jurisdictions.

2. Current transfer mechanics need to be reviewed to assess compliance with GDPR and, where necessary, remedial steps implemented before GDPR comes into force.

3. For intra-group transfers, consider binding corporate rules which not only provide a good basis for transfers but also help demonstrate broader compliance with GDPR helping to comply with the principle of accountability.

H. DATA BREACH NOTIFICATION

One of the most profound changes to be introduced by GDPR is a European wide requirement to notify data breaches to supervisory authorities and affected individuals.

In the US, data breach notification laws are now in force in all 50 States and the hefty penalties for failing to notify have fundamentally changed the way US organizations investigate and respond to data incidents. Not notifying has become a high risk option.

In contrast, Europe previously had no universally applicable law requiring notification of breaches. In the majority of Member States there was either no general obligation to notify or minimal sanctions for failing to do so; for many organizations not notifying and thereby avoiding the often damaging media fall-out is still common practice in Europe. That fundamentally changes with GDPR in force.

GDPR requires "the controller without undue delay, and where feasible, not later than 72 hours after having become aware of it, [to] notify the … breach to the supervisory authority" (Article 33(1)). When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals the controller is also required to notify the affected individuals "without undue delay" (Article 34). Processors are required to notify the controller without undue delay having become aware of the breach (Article 33(2)).

The notification to the regulator must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's DPO or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Although the obligation to notify is conditional on awareness, burying your head in the sand is not an option as controllers are required to implement appropriate technical and organizational measures together with a process for regularly testing, assessing and evaluating the effectiveness of those measures to ensure the security of processing (Article 32). Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits by the supervisory authority.

Failing to comply with the articles relating to security and data breach notification attract fines of up to 10 million Euros or 2% of annual worldwide turnover, potentially for both the controller and the processor. As data breach often leads to investigations by supervisory authorities and often uncovers other areas of non-compliance, it is quite possible that fines of up to 20 million Euros or 4% of annual worldwide turnover will also be triggered.

Practical implications

1. Notification will become the norm: Sweeping breaches under the carpet has become a very high risk option under GDPR. Organizations that are found to have deliberately not notified can expect the highest fines and lasting damage to corporate and individual reputations. Notifying and building data breach infrastructure to enable prompt, compliant notification will be a necessity under GDPR.

2. A coordinated approach, including technology, breach response policy and training and wider staff training. Data breaches are increasingly a business as usual event. Lost or stolen devices; emails sent to incorrect addresses in error and the continuing rise of cybercrime means that for many organizations, data breaches are a daily occurrence. To deal with the volume of breaches,

organization's need a combination of technology, breach response procedures and staff training.

a. Technology requirements: these will vary for each organization but will typically include a combination of firewalls, log recording, data loss prevention, malware detection and similar applications. There are an increasingly sophisticated array of applications that learn what "normal" looks like for a particular corporate network to be able to spot unusual events more effectively. The state of the art continues to change rapidly as organizations try to keep pace with sophisticated hackers. Regular privacy impact assessments and upgrades of technology are required.
b. Breach response procedures: to gain the greatest protection from technology, investment is required in dealing with red flags when they are raised by internal detection systems or notified from external sources. Effective breach response requires a combination of skill sets including IT, PR and legal. Develop a plan and test it regularly.
c. Staff training: the weak link in security is frequently people rather than technology. Regular staff training is essential to raise awareness of the importance of good security practices, current threats and who to call if a breach is suspected. It is also important to avoid a blame culture that may deter staff from reporting breaches.

3. Consider privilege and confidentiality as part of your plan. Make sure that forensic reports are protected by privilege wherever possible to avoid compounding the losses arising from a breach. Avoid the temptation to fire off emails when a breach is suspected; pick up the phone. Don't speculate on what might have happened; stick to the facts. Bear in mind that you may be dealing with insider threat – such as a rogue employee – so keep any investigation on a strictly need to know basis and always consider using external investigators if there is any possibility of an inside attack.

4. Appoint your external advisors today if you haven't done so already. When a major incident occurs, precious time can be wasted identifying and then retaining external support teams when you are up against a 72 hour notification deadline. Lawyers, forensics and PR advisors should ideally be contracted well before they are needed for a live incident. Find out more about DLA Piper's breach response credentials and team.

5. Insurance: many insurers are now offering cyber insurance. However, there is a lack of standardization in coverage offered. Limits are often too small for the likely exposure. Conditions are often inappropriate such as a requirement for the insured to have fully complied with all applicable laws and its own internal policies which will rarely be the case. That said, it is usually possible to negotiate better coverage with carriers in what continues to be a soft insurance market. Now is a good time to check the terms of policies and work with your legal team and brokers to ensure that you have the best possible coverage. You should clarify with brokers and underwriters what amounts to a notifiable incident to insurers under your policies as again there is no common standard and failing to notify when required may invalidate cover. You should also ensure that your insurance policies will cover the costs of your preferred external advisors as many policies will only cover advice from panel advisors.

6. Develop standard notification procedures: Perhaps the greatest challenge facing organizations and regulators is the sheer volume of data breach and the lack of standards or guidance as to how breaches should be notified and at what point they become notifiable. In the absence of guidance organization's will need to make an informed decision as to how to develop internal operations for the detection, categorization, investigation, containment and reporting of data breaches. Similarly, supervisory authorities will need to develop standard approaches and standard categorizations of incidents to ensure that limited resources are focused on the most serious incidents first.

I. MORE RIGHTS FOR INDIVIDUALS

GDPR builds on the rights enjoyed by individuals under the previous Directive, enhancing those rights and introducing a new right to data portability. These rights are backed up with provisions making it easier to claim damages for compensation and for consumer groups to enforce rights on behalf of consumers.

Transparency

One of the core building blocks of GDPR's enhanced rights for individuals is the requirement for greater transparency. Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data is obtained:

- the identity and contact details of the controller
- the Data Protection Officer's contact details (if there is one)
- both the purpose for which data will be processed and the legal basis for processing including if relevant the legitimate interests for processing
- the recipients or categories of recipients of the personal data
- details of international transfers
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- the existence of rights of the data subject including the right to access, rectify, require erasure (the "right to be forgotten"), restrict processing, object to processing and data portability; where applicable the right to withdraw consent, and the right to complain to supervisory authorities
- the consequences of failing to provide data necessary to enter into a contract
- the existence of any automated decision making and profiling and the consequences for the data subject.
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Slightly different transparency requirements apply (Article 14) where information have not been obtained from the data subject.

Subject access rights (Article 15)

These broadly follow the existing regime set out in the Directive though some additional information must be disclosed and there is no longer a right for controllers to charge a fee, with some narrow exceptions. Information requested by data subjects must be provided within one month as a default with a limited right for the controller to extend this period for up to three months.

Right to rectify (Article 16)

Data subjects continue to enjoy a right to require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure (right to be forgotten)(Article 17)

This forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right to be forgotten now has its own Article in GDPR. However, the right is not absolute; it only arises in quite a narrow set of circumstances notably where the controller has no legal ground for processing the information. As demonstrated in the Google Spain decision itself, requiring a search engine to remove search results does not mean the underlying content controlled by third party websites will necessarily be removed. In many cases the controllers of those third party websites may have entirely legitimate grounds to continue to process that information, albeit that the information is less likely to be found if links are removed from search engine results.

The practical impact of this decision has been a huge number of requests made to search engines for search results to be removed raising concerns that the right is being used to remove information that it is in the public interest to be accessible.

Right to restriction of processing (Article 18)

Data subjects enjoys a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data is no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller and whether these override those of the data subject are contested.

Right to data portability (Article 20)

This is an entirely new right in GDPR and has no equivalent in the previous Directive. Where the processing of personal data is justified either on the basis that the data subject has given their consent to processing or where processing is necessary for the performance of a contract, or where the processing is carried out be automated means, then the data subject has the right to

receive or have transmitted to another controller all personal data concerning them in a structured, commonly used and machine-readable format.

The right is a good example of the regulatory downsides of relying on consent or performance of a contract to justify processing – they come with various baggage under GDPR relative to other justifications for processing.

Where the right is likely to arise controllers need to develop procedures to facilitate the collection and transfer of personal data when requested to do so by data subjects.

Right to object (Article 21)

The Directive's right to object to the processing of personal data for direct marketing purposes at any time is retained.

In addition, data subjects have the right to object to processing which is legitimized on the grounds either of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject or that the processing is for the establishment, exercise or defense of legal claims.

The right not to be subject to automated decision making, including profiling (Article 22)

This right expands the Directive right not to be subject to automated decision making. GDPR expressly refers to profiling as an example of automated decision making. Automated decision making and profiling "which produces legal effects concerning [the data subject] … or similarly significantly affects him or her" are only permitted where

(a) necessary for entering into or performing a contract
(b) authorized by EU or Member State law, or
(c) the data subject has given their explicit (i.e. opt-in) consent.

The scope of this right is potentially extremely broad and may throw into question legitimate profiling for example to detect fraud and cybercrime. It also presents challenges for the online advertising industry and website operators who will need to revisit consenting mechanics to justify online profiling for behavioral advertising. This is an area where further guidance is needed on how Article 22 will be applied to specific types of profiling.

Practical implications

1. Controllers need to review and update current fair collection notices to ensure compliance with the expanded information requirements. Much more granular notices are required using plain and concise language.

2. Consideration should be given to which legal justifications for processing are most appropriate for different purposes, given that some such as consent and processing for performance of a contract come with additional regulatory burden in the form of enhanced rights for individuals.

3. For some controllers with extensive personal data held on consumers, it is likely that significant investment in customer preference centers is required on the one hand to address enhanced transparency and choice requirements and on the other hand to automate compliance with data subject rights.

4. Existing data subject access procedures should be reviewed to ensure compliance with the additional requirements of GDPR.

5. Policies and procedures need to be written and tested to ensure that controllers are able to comply with data subjects' rights within the time limits set by GDPR. In some cases, such as where data portability engages, significant investments may be required.

J. DATA PROTECTION OFFICERS

GDPR introduces a significant new governance burden for those organizations which are caught by the new requirement to appoint a DPO. Although this was already a requirement for most controllers in Germany under previous data protection laws, it is an entirely new requirement (and cost) for many organizations.

The following organizations must appoint a data protection officer (DPO) (Article 37):

- public authorities
- controllers or processors whose core activities consist of processing operations which by virtue of their nature, scope or purposes require regular and systemic monitoring of data subjects on a large scale
- controllers or processors whose core activities consist of processing sensitive personal data on a large scale.

DPOs must have "expert knowledge" (Article 37(5)) of data protection law and practices though perhaps in recognition of the current shortage of experienced data protection professionals, it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "properly and in a timely manner in all issues which relate to the protection of personal data" (Article 38(1)). The role is therefore a sizeable responsibility for larger controllers and processors.

The DPO must directly report to the highest management level, must not be told what to do in the exercise of their tasks and must not be dismissed or penalized for performing their tasks (Article 38(3)).

The specific tasks of the DPO are set out in GDPR including (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws
- to monitor compliance with law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- to advise and monitor data protection impact assessments
- to cooperate and act as point of contact with the supervisory authority

Practical implications

1. Organizations need to assess whether or not they fall within one or more of the categories where a DPO is mandated. Public authorities will be caught (with some narrow exceptions) as will many social media, search and other tech firms who monitor online consumer behavior to serve targeting advertising. Many b2c businesses which regularly monitor online activity of their customers and website visitors will also be caught.

2. There is currently a shortage of expert data protection officers as outside of Germany this is a new requirement for most organizations. Organizations will therefore need to decide whether to appoint an internal DPO with a view to training them up over the next couple of years or use one of the external DPO service providers several of which have been established to fill this gap in the market. Organizations might consider a combination of internal and external DPO resources as given the size of the task it may not be realistic for just one person to do it.

K. ACCOUNTABILITY AND GOVERNANCE

Accountability is a recurring theme of GDPR. Data governance is no longer just a case of doing the right thing; organizations need to be able to prove that they have done the right thing to regulators, to data subjects and potentially to shareholders and the media often years after a decision was taken.

GDPR requires each controller to demonstrate compliance with the data protection principles (Article 5(2)). This general principle manifests itself in specific enhanced governance obligations which include:

- ***Keeping a detailed record of processing operations*** (Article 30)
  The requirement in previous data protection laws to notify the national data protection authority about data processing operations was abolished and replaced by a more general obligation on the controller to keep extensive internal records of their data protection activities. The level of detail required is far more granular compared to many previous Member State notification requirements. There is some relief granted to organizations employing fewer than 250 people though the exemption is very narrowly drafted.
- ***Performing data protection impact assessment for high risk processing*** (Article 35)
  A data protection impact assessment is a mandatory pre-requisite before processing personal data for processing which is

likely to result in a high risk to the rights and freedoms of individuals. Specific examples are set out of high risk processing requiring impact assessments including: automated processing including profiling that produce legal effects or similarly significantly affect individuals; processing of sensitive personal data; and systematic monitoring of publicly accessible areas on a large scale. DPOs, where in place, have to be consulted. Where the impact assessment indicates high risks in the absence of measures to be taken by the controller to mitigate the risk, the supervisory authority must also be consulted (Article 36) and may second guess the measures proposed by the controller and has the power to require the controller to impose different or additional measures (Article 58).

- ***Designating a data protection officer*** (Article 37) See Data Protection Officers
- ***Notifying and keeping a comprehensive record of data breaches*** (Articles 33 and 34) See Data Breach Notification
- ***Implementing data protection by design and by default*** (Article 25)
  GDPR introduces the concepts of "data protection by design and by default." "Data protection by design" requires taking data protection risks into account throughout the process of designing a new process, product or service, rather than treating it as an afterthought. This means assessing carefully and implementing appropriate technical and organizational measures and procedures from the outset to ensure that processing complies with GDPR and protects the rights of the data subjects.
  "Data protection by default" requires ensuring mechanisms are in place within the organization to ensure that, by default, only personal data which are necessary for each specific purpose are processed. This obligation includes ensuring that only the minimum amount of personal data is collected and processed for a specific purpose; the extent of processing is limited to that necessary for each purpose; the data is stored no longer than necessary and access is restricted to that necessary for each purpose.

Practical implications

1. Data mapping: every controller and processor needs to carry out an extensive data audit across the organization and supply chains, record this information in accordance with the requirements of Article 30 and have governance in place to ensure that the information is kept up-to-date. The data mapping exercise is also be crucial to be able to determine compliance with GDPR's other obligations so this exercise should be commenced as soon as possible.

2. Gap analysis: Once the data mapping exercise is complete, each organization needs to assess its current level of compliance with the requirements of GDPR. Gaps need to be identified and remedial actions prioritized and implemented.

3. Governance and policy for data protection impact assessments: the data mapping exercise should identify high risk processing. Data protection impact assessments need to be completed and documented for each of these (frequently these will include third party suppliers) and any remedial actions identified implemented. Supervisory authorities may need to be consulted. A procedure needs to be put in place to standardize future data protection impact assessments and to keep existing impact assessments regularly updated where there is a change in the risk of processing.

4. Data protection by design and by default: in part these obligations will be addressed through implementing remedial steps identified by the gap analysis and in data protection impact assessments. However, to ensure that data protection by design and by default is delivered, extensive staff and supplier engagement and training will also be required to raise awareness of the importance of data protection and to change behaviors.

L. DEROGATIONS

European data protection laws today are in many cases substantively very different among Member States. This is partly due to the ambiguities in the Directive being interpreted and implemented differently, and partly due to the Directive permitting Member States to implement different or additional rules in some areas. As GDPR will become law without the need for any secondary implementing laws, there will be a greater degree of harmonization relative to the current regime. However, GDPR preserves the right for Member States to introduce different laws in many important areas and as a result we are likely to continue to see a patchwork of different data protection laws among Member States, for certain types of processing.

Each Member State is permitted to restrict the rights of individuals and transparency obligations (Article 23) by legislation when the restriction "respects the essence of fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" to safeguard one of the following:

(a) national security
(b) defense
(c) public security
(d) the prevention, investigation, detection or prosecution of breaches of ethics for regulated professions, or crime, or the execution of criminal penalties
(e) other important objectives of general public interest of the EU or a Member State, in particular economic or financial interests
(f) the protection of judicial independence and judicial proceedings
(g) a monitoring, inspection or regulatory function connected with national security, defense, public security, crime prevention, other public interest or breach of ethics
(h) the protection of the data subject or the rights and freedoms of others
(i) the enforcement of civil law claims

To be a valid restriction for the purposes of GDPR, any legislative restriction must contain specific provisions setting out:

(a) the purposes of processing
(b) the categories of personal data
(c) the scope of the restrictions
(d) the safeguards to prevent abuse or unlawful access or transfer
(e) the controllers who may rely on the restriction
(f) the permitted retention periods
(g) the risks to the rights and freedoms of data subjects
(h) the right of data subjects to be informed about the restriction, unless prejudicial to the purpose of the restriction

In addition to these permitted restrictions, Chapter IX of GDPR sets out various specific processing activities which include additional derogations, exemptions and powers for Member States to impose additional requirements. These include:

- processing and freedom of expression and information (Article 85)
- processing and public access to official documents (Article 86)
- processing of national identification numbers (Article 87)
- processing in the context of employment (Article 88)
- safeguards and derogations to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 89)
- obligations of secrecy (Article 90)
- existing data protection rules of churches and religious associations (Article 91)

These special cases also appeared in the Directive, though in some cases have been amended or varied in GDPR.

Practical implications

1. Controllers and processors first need to determine which Member States' laws apply to their processing activities and whether processing will be undertaken within any specific processing activities which may be subject to additional restrictions.

2. These Member State laws then need to be checked to determine what additional requirements engage. Changes in law need to be monitored and any implications for processing activities addressed.

3. Derogations pose a challenge to multi-national organizations seeking to implement standard European-wide solutions to address compliance with GDPR; these need to be sufficiently flexible to allow for exceptions where different rules engage in one or more Member State.

M. CROSS-BORDER ENFORCEMENT

The ideal of a one-stop-shop ensuring that controllers present in multiple Member States would only have to answer to their lead home regulator failed to make it into the final draft. GDPR includes a complex, bureaucratic procedure allowing multiple

'concerned' authorities to input into the decision making process.

The starting point for enforcement of GDPR is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities and there are powers for a supervisory authorities in another Member State to enforce where infringements occur on its territory or substantially affects data subjects only in its territory (Article 56(2)).

In situations where multiple supervisory authorities are involved in an investigation or enforcement process there is a cooperation procedure (Article 60) involving a lengthy decision making process and a right to refer to the consistency mechanism (Articles 63 - 65) if a decision cannot be reached, ultimately with the European Data Protection Board having the power to take a binding decision.

There is an urgency procedure (Article 66) for exceptional circumstances which permits a supervisory authority to adopt provisional measures on an interim basis where necessary to protect the rights and freedoms of data subjects.

Practical implications

1. Controllers and processors need to determine which Member States' supervisory authorities have jurisdiction over their processing activities; which is the lead authority and which other supervisory authorities may have jurisdiction.

2. An important aspect of managing compliance risk is to try to stay on the right side of your regulator by engaging positively with any guidance published and taking up opportunities such as training and attending seminars.

KEY CONTACTS

Prof. Patrick Van Eecke
Partner
T +32 2 500 1630
patrick.van.eecke@dlapiper.com

DATA PROTECTION AND PRIVACY GROUP KEY CONTACTS

Americas

Jim Halpert
Partner & Chair of US Data Protection and Privacy Group
T +1 202 799 4441
jim.halpert@dlapiper.com

Jennifer Kashatus
Partner, Data Protection, Privacy and Security
T +1 202 799 4448
jennifer.kashatus@dlapiper.com

Europe, Middle East and Africa

Andrew Dyson
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +44 (0)113 369 2403
andrew.dyson@dlapiper.com

Prof. Patrick Van Eecke
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +32 2 500 1630
patrick.van.eecke@dlapiper.com

Denise Lebeau-Marianna
Partner, Head of Data Protection Practice - EuroPriSe Expert
T + 33 (0)1 40 15 24 98
denise.lebeau-marianna@dlapiper.com

Diego Ramos
Partner
T +349 17901658
diego.ramos@dlapiper.com

Richard van Schaik
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +31 20 541 9828
richard.vanschaik@dlapiper.com

Asia Pacific

Nicholas Boyle
Partner
T +61 2 9286 8479
nicholas.boyle@dlapiper.com

Scott Thiel
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +852 2103 0519
scott.thiel@dlapiper.com

EDITORS

Kate Lucente
Partner and Co-Editor,

James Clark
Associate and

Data Protection Laws of
World Handbook
T +1 813 222 5927
kate.lucente@dlapiper.com

Co-Editor, Data
Protection Laws of the
World Handbook
T +44 113 369 2461
james.clark@dlapiper.com

ANGOLA

Last modified 20 May 2019

LAW

Angola regulates data privacy and protection issues under the Data Protection Law (Law no. 22/11, 17 June 2011), the Electronic Communications and Information Society Services Law (Law no. 23/11, 20 June 2011) and the Protection of Information Systems and Networks Law (Law no. 7/17, 16 February 2017).

DEFINITIONS

Definition of personal data

The Data Protection Law defines personal data as any given information, regardless of its nature, including images and sounds related to a specific or identifiable individual.

An identifiable person is an individual directly or indirectly identified, notably, by reference to his or her identification number or to the combination of specific elements of his or her physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

The Data Protection Law defines sensitive personal data as personal data related to:

- Philosophical or political beliefs
- Political affiliations or trade union membership
- Religion
- Private life
- Racial or ethnic origin
- Health or sex life (including genetic data)

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Law establishes the *Agência de Proteção de Dados* (APD) as Angola's data protection authority. Although Presidential Decree 214/2016 (currently in force) approved the APD's Organic Statute in October 2016, the APD has not yet been created.

REGISTRATION

Once it is created, entities will be required to provide prior notice to, or obtain prior authorization from, APD (depending on the type of personal data and purpose of processing) to process personal data. Please note that in the case of authorization, compliance with specific legal conditions is mandatory. APD has authority to exempt certain processing from notification

requirements.

Generally, notification and authorization requests should include the following:

- The name and address of the controller and of its representative (if applicable)
- The purposes of the processing
- A description of the data subject categories and the personal data related to those categories
- The recipients or under which categories of recipient to whom the personal data may be communicated and respective conditions
- Details of any third party entities responsible for the processing
- The possible combinations of personal data
- The duration of personal data retention
- The process and conditions for data subjects to execute further rights of access, rectification, deletion, opposition and updating
- Any predicted transfers of personal data to third countries
- A general description (to allow APD to assess whether security measures adopted are suitable to protect personal data in its processing)

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

Generally, entities must obtain prior express consent from data subjects and provide prior notice to the APD to lawfully collect and process personal data. However, data subject consent is not required in certain circumstances provided by law.

To lawfully collect and process sensitive personal data, a legal provision must allow for processing and entities must obtain prior authorization from APD (please note that the authorization may only be granted in specific cases provided by law). If sensitive personal data processing results from a legal provision, APD must be provided with notice.

All data processing must follow these general principles: transparency, legality, good faith, proportionality, truthfulness and respect to private life as well as to legal and constitutional guarantees.

It is also mandatory that data processing is limited to the purpose for which the data is collected and that personal data is not held for longer than is necessary for that purpose.

There are specific rules applicable to the processing of personal data related to the following:

- Sensitive data on health and sexual life
- Illicit activities, crimes and administrative offenses
- Solvency and credit data
- Video surveillance and other electronic means of control
- Advertising by email
- Advertising by electronic means (direct marketing)
- Call recording

Specific rules for the processing of personal data within the public sector also apply.

TRANSFER

International transfers of personal data to countries with an adequate level of protection require prior notification to the APD. An adequate level of protection is understood as a level of protection equal to the Angolan Data Protection Law. APD decides which countries ensure an adequate level of protection by issuing an opinion to this respect.

International transfers of personal data to countries that do not ensure an adequate level of protection are subject to prior

authorization from the APD, which will only be granted if specific requirements are met. For transfers between companies in the same group, the requirement of an adequate level of protection may be reached through the adoption of harmonized and mandatory internal rules on data protection and privacy.

Please note that the communication of personal data to a recipient, a third party or a subcontracted entity is subject to specific legal conditions and requirements.

SECURITY

Data controllers must implement appropriate technical and organizational measures and adopt adequate security levels to protect personal data from accidental or unlawful total or partial destruction, accidental loss, total or partial alteration, unauthorized disclosure or access (in particular where the processing involves the transmission of data over a network) and against all other unlawful forms of processing.

Such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, relative to the entities facilities and implementation costs. Specific security measures shall be adopted regarding certain type of personal data and purposes (notably, sensitive data, call recording and video surveillance).

Under the Protection of Information Systems and Networks Law, service providers, operators and companies offering information society services must: (i) guarantee the security of any device or set of devices used in the storage, processing, recovery or transmission of computer data on execution of a computer program and (ii) promote the registration of users as well as the implementation of technical measures in order to anticipate, detect and respond to risk situations. The Law requires an accident and incident management plan in case of a computer emergency.

BREACH NOTIFICATION

There is no mandatory breach notification requirement under the Data Protection Law.

However, pursuant to the Electronic Communications and Information Society Services Law, companies offering electronic communications services accessible to the public shall, without undue delay, notify the APD and the Electronic Communications Authority, *Instituto Angolano das Comunicações*, (INACOM) of any breach of security committed with intent or that recklessly leads to destruction, loss, partial or total modification or non-authorized access to personal data transmitted, stored, retained or in any way processed under the offer of electronic communications services.

Companies offering electronic communications services accessible to the public shall also keep an accurate register of data breaches, indicating the concrete facts and consequences of each breach and the measures put in place to repair or prevent the breach.

The same applies under Protection of Information Systems and Networks Law.

ENFORCEMENT

Data protection

As mentioned above, the competent authority for the enforcement of Data Protection Law is the APD. However, considering that the APD is not yet created, the level of enforcement is not significant at this stage.

Electronic communications

INACOM regulates and monitors compliance with the Electronic Communications and Information Society Services Law, and issues penalties for its violation. Unlike the APD, the INACOM has been created, however, its level of enforcement is not yet significant.

ELECTRONIC MARKETING

The dissemination of electronic communications for advertising purposes is generally subject to the prior express consent of its

recipient (opt-in) and to prior notification to APD.

Entities may process personal data for electronic marketing purposes without data subject consent in specific circumstances, notably:

- When advertising is addressed to the data subject as representative employee of a corporate person, and
- When advertising communications are sent to an individual with whom the product or service supplier has already concluded a transaction, provided an opportunity to refuse consent was expressly provided to the customer at the time of the transaction at no additional cost.

ONLINE PRIVACY

The Electronic Communications and Information Society Services Law establishes the right of all Citizens to enjoy protection against abuse or violations of their rights through the Internet or other electronics means, such as:

- The right to confidentiality of communications and to privacy and non-disclosure of their data
- The right to security of their information by improvement of quality, reliability and integrity of the information systems
- The right to security on the Internet, specifically for minors
- The right not to receive spam
- The right to the protection and safeguarding of their consumer rights and as users of networks or electronic communications services

In view of the above, entities are generally prohibited from storing any kind of personal data without prior consent of the user. This does not prevent technical storage or access for the sole purpose of carrying out the transmission of a communication over an e-communication network or if strictly necessary in order for the provider of an information society service to provide a service expressly requested by the subscriber or user.

Traffic data

The processing of traffic data is allowed when required for billing and payment purposes, but processing is only permitted until the end of the period during which the bill may lawfully be challenged or payment pursued. Traffic data must be eliminated or made anonymous when no longer needed for the transmission of the communication.

The storage of specific information and access to that information is only allowed on the condition that the subscriber or user has provided his or her prior consent. The consent must be based on accurate, clear and comprehensive information, namely about the type of data processed, the purposes and duration of the processing and the availability of data to third parties in order to provide value added services.

Electronic communications operators may store traffic data only to the extent required and for the time necessary to market electronic communications services or provide value added services. Prior express consent is required and such consent may be withdrawn at any time.

Processing should be limited to those employees in charge of:

- Billing or traffic management
- Customer inquiries
- Fraud detection
- Marketing of electronic communications
- Services accessible to the public
- The provision of value added services

Notwithstanding the above, electronic communication operators should keep in an autonomous file all traffic and localization data exclusively for the purpose of:

- Investigation
- Detection, or

- Prosecution of criminal offenses on Information and Communication Technologies (ICT)

Location data

Location Data processing is only allowed if the data is made anonymous or to the extent and for the duration necessary for the provision of value added services, provided prior express consent is obtained. In this case, prior complete and accurate information must be provided on the type of data being processed, as well as the purposes and duration of processing and any possibility of disclosure to third parties for the provision of value added services.

Electronic communication operators must ensure that data subjects have the opportunity to withdraw consent, or temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication, at any time. The withdrawal mechanism must be provided through simple means, free of charge to the user. Processing should be limited to those employees in charge of electronic communications services accessible to the public.

KEY CONTACTS

VCA – Law Firm
www.vca-angola.com

Orlanda Vuite
Associate
ADCA Advogados Angola
T +244 926 61 25 25
o.vuite@adca-angola.com

Carmina Cardoso
Of Counsel
T +244 926 61 25 25
c.cardoso@vca-angola.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ARGENTINA

Last modified 28 January 2019

LAW

Article 43 of the Federal Constitution, third paragraph, provides, in relevant part that any person may file an action to have access to personal data about such person and to information about the purpose with which they are kept, included in public data registries or banks, or in private data registries or banks, and to request the suppression, correction, confidentiality or updating of the data where inaccurate or discriminatory.

These provisions do not create an express constitutional right to privacy or data protection, but do create the basic framework for the protection of such right, as well as the foundation for the legislation, subsequently enacted, which regulates the details of that protection.

Law 25,326 - the Personal Data Protection Law (PDPL) includes the basic personal data rules. It follows international standards, and has been considered as granting adequate protection by the European Commission. Decree 1558 of 2001 includes regulations issued under the PDPL. Further regulations have been issued by the relevant agencies.

DEFINITIONS

Definition of personal data

Personal data is defined as information of any type referred to individuals or legal entities, determined or which may be determined.

Definition of sensitive personal data

Sensitive data includes personal data which reveal racial or ethnic origin, political opinions, religious, philosophical or moral convictions, trade union affiliation and information related to health and sexual activities.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to Decree 746 of 2017, it is the Agency for Access to Public Information (Agencia de Acceso a la Información Pública).

REGISTRATION

All archives, registries, databases and data banks, whether public or private, having the purpose of supplying information, must be registered with the Registry organized by the national data protection authority. This registration requires the following information, to be provided to the registry:

- The name and domicile of the person responsible for the archive, registry, database or data bank
- The characteristics and purpose of the archive, registry, database or data bank

- The nature of the personal data included or to be included in the archive, registry, database or data bank
- The way in which data are collected and updated
- The destination of the data and the identity of the individuals or legal entities to whom such data may be transferred
- The way in which the recorded information is interrelated
- The means to assure the security of the data, indicating the category of persons with access to the processing of data
- The term during which the data will be preserved
- The way and conditions pursuant to which interested persons may have access to the data referring to such persons, and the procedures to be followed to rectify and update the registered data

DATA PROTECTION OFFICERS

Generally, there is no specific requirement to appoint a data protection officer. Under certain circumstances, in which special security standards apply, it may be necessary to appoint an officer in charge of data security.

COLLECTION & PROCESSING

Personal data collected for purposes of processing must be truthful, adequate, relevant and not excessive in relation with the scope and purpose for which they were obtained. The gathering of data shall not take place by unfair or fraudulent means or in an otherwise illegal manner.

Personal data may not be used for purposes different from or incompatible with those for which the personal data was initially collected. Personal data must be accurate and properly updated when necessary. Totally or partially inaccurate personal data, or those that are incomplete, shall be suppressed and substituted, or completed where relevant, by the person responsible for the archive or database, whenever such person becomes aware of the inaccurate or incomplete character of the information.

Consent from the data subject is required, which must be free, express and informed consent and in writing or in another equivalent form, unless:

- The personal data were obtained from sources open to unrestricted public access
- The personal data were obtained as part of the performance of state duties or in compliance with a legal obligation
- The personal data consists of lists whose data are limited to the name, national identity document number, tax or social security identification, occupation, date of birth and domicile
- The personal data are derived from a contractual, scientific or professional relationship and are necessary for such relationship
- The personal data result from operations conducted by financial entities with their clients or consist in the information such financial entities receive from their clients pursuant to the Financial Entities Law

When the authorization for the collection and processing of data is requested, the data subject must be informed about the purpose for which the data will be processed, as well as about the individuals or groups of individuals who will have access to the processed information. In addition, the archive, registry or data bank where the information will be kept must be identified, together with the person responsible for it. The data subject must be informed about the voluntary or compulsory nature of the answers requested from such owner, as well as about the consequences of providing the personal data or of refusing to give such information or of providing untruthful information. The data subject must also be informed about the right to access, rectify and suppress the relevant data.

Special rules apply to sensitive data. No person may be required to disclose sensitive data. Sensitive data may only be collected

and processed where necessary, and with consent, as expressly permitted by law, or for statistical or scientific purposes provided the person they refer to may not be identified.

Data related to criminal records may only be processed by the relevant public authorities.

TRANSFER

Transfers and disclosures to third parties

Personal data may only be transferred for legitimate purposes of the transferor and the transferee, and generally with the prior consent of the data subject who must be informed of the transfer's purpose and of the transferee's identity. This consent may be rescinded.

Consent is not required in the case of transfer of data regarding which consent was not necessary for collection. Also, it is not necessary in the case of transfer of data between state agencies, for purposes of performance of their respective activities, on in connection with health-related data, if the transfer is necessary for public health or emergency reasons, or for the performance of epidemiological studies, provided the identity of the persons to whom such data refer is reserved by means of adequate dissociation mechanism. In addition, consent is not necessary, for personal data generally, if an adequate dissociation mechanism is used in a way such that the data subjects are not identifiable.

Cross-border transfers

The cross-border transfer of personal data is prohibited to countries or international or supranational organization which do not provide adequate protection to such data, unless:

- The data subjects expressly consents to that transfer
- The transfer is necessary for international judicial cooperation
- The transfer takes place as part of certain exchanges of medical data
- Bank or stock exchange transfers, in the context banking or stock exchange transactions
- The transfer takes place as provided in the context of international treaties to which Argentina is a party
- The transfer has as its purpose the international cooperation between intelligence agencies engaged in combating organized crime, terrorism and drug traffic

SECURITY

The person responsible for a data archive, or using such archive, must adopt the technical and organizational measures to assure the security and confidentiality of personal data, so as to avoid their adulteration, loss, consultation or non-authorized processing, and to detect the misuse of information. The recording of personal data in archives, registries or data banks that do not comply with the legal requirements on integrity and security is prohibited.

BREACH NOTIFICATION

Not specifically required under data protection law.

Failure to notify a data security breach is not in itself a violation of the data protection regime, but may bear on the effects of security violation, especially if lack of such notification results in other security breaches or damages. The person responsible for the data must keep records on security breaches, and these records may be requested by the data protection authority.

Breach notification may be mandatory if the data protection authority specifically requests information about data breaches.

ENFORCEMENT

There are several enforcement mechanisms:

- The data protection authority may enforce the legal provisions and regulations on data protection, imposing fines in case of violation.
- Violation of data protection rules may constitute a crime subject to prison terms imposed by criminal courts.
- Court actions may be brought to have access to personal data and to request their correction, suppression, confidentiality or updating.

ELECTRONIC MARKETING

Electronic marketing, to the extent that it may involve processing of personal data, is subject to the general rules applicable to such data, such as valid data subject consent, adequate privacy notices as to use and disclosure of personal data and data subject rights.

ONLINE PRIVACY

Although there are no detailed regulations on online privacy, the general rules on privacy provided by the Civil and Commercial Code are applicable in this context. Nuisances from unrequested communications may be actionable. Unauthorized collection of personal data will be subject to the general rules applicable to such data.

KEY CONTACTS

Guillermo Cabanellas
Senior Partner
T +5411 41145500
g.cabanellas@dlapiper.com.ar

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

AUSTRALIA

Last modified 28 January 2019

LAW

Australia regulates data privacy and protection through a mix of federal, state and territory laws. The Federal Privacy Act 1988 (Cth) (Privacy Act) and its Australian Privacy Principles (APPs) apply to private sector entities with an annual turnover of at least AU$3 million, and all Commonwealth Government and Australian Capital Territory Government agencies.

Under the Privacy Act, the Privacy Commissioner has authority to conduct investigations, including own motion investigations, to enforce the Privacy Act and seek civil penalties for serious and egregious breaches or for repeated breaches of the APPs where an entity has failed to implement remedial efforts.

Most states and territories in Australia (except Western Australia and South Australia) have their own data protection legislation applicable to state government agencies, and private businesses that interact with state government agencies. These acts include:

- Information Privacy Act 2014 (Australian Capital Territory)
- Information Act 2002 (Northern Territory)
- Privacy and Personal Information Protection Act 1998 (New South Wales)
- Information Privacy Act 2009 (Queensland)
- Personal Information Protection Act 2004 (Tasmania), and
- Privacy and Data Protection Act 2014 (Victoria)

Additional parts of state and federal legislation relate to data protection. For example, the following all impact privacy and data protection for specific types of data or specific activities: the Telecommunications Act 1997 (Cth), the Criminal Code Act 1995 (Cth), the National Health Act 1953 (Cth), the Health Records and Information Privacy Act 2002 (NSW), the Health Records Act 2001 (Vic) and the Workplace Surveillance Act 2005 (NSW).

Further, specific regulators have expressed an expectation that regulated entities should have specified data protection in place. For example, the Australian Prudential and Regulatory Authority regulates financial services institutions, and the Australian Securities and Investment Commission regulates corporations generally.

Notably, both the Australian Commonwealth and state governments have expressed an intent to further consider data privacy and protection issues beyond existing legislation, including a focus on protecting minors online. However, the focus of this entry relates to the application of the Privacy Act to private sector entities, which are referred to as "organizations."

Under the Privacy Act and the APPs, an organization can be any of the following:

- An individual

- A body corporate
- A partnership
- Any other unincorporated association
- A trust

Other important privacy and data protection laws

Assistance and Access Act

The federal parliament also passed with great urgency in late 2018 a very wide ranging omnibus amendment act (Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)) which, ostensibly, provides law enforcement agencies with access to encrypted data for serious crime investigation. However, the legislation may inadvertently have a much broader remit with limited judicial oversight, and the legislation has been the subject of much criticism from local and global technology firms which have stated the legislation has the potential of significantly impacting on security/encryption solutions in Australia. The enacted laws are ambiguous in many areas, and it is likely that the legislation will be further amended in early 2019, reflecting a further review of the operation of the Act by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and with changes including, among other things, the re-wording of several key definitions and the omission of others.

At its heart, the Act allows various agencies to any of the following:

- Issue a "technical assistance notice," which will require a communications provider to give assistance that is reasonable, proportionate, practicable and technically feasible
- Issue a "technical capability notice," which will require a communications provider to build new capabilities to assist. The Attorney-General must consult with the communications provider prior to issuing the notice, and must be satisfied that the notice is reasonable, proportionate, practicable and technically feasible
- Make "technical assistance requests," to give foreign and domestic communications providers and device manufacturers a legal basis to provide voluntary assistance to various Australian intelligence organizations and interception agencies relating to issues of national interest, national security and law enforcement

Organizations will need to ensure customer terms and conditions deal carefully with the matter of legal compliance and any commitments made to customers generally.

Consumer Data Right

Following a number of policy reviews including the Productivity Commission's "Data Availability and Use" report and the "Review into Open Banking in Australia," the Commonwealth Government also committed to implement a Consumer Data Right (CDR) in Australia. The regime to implement the CDR has not yet been legislation, although the current draft bill seeks to implement the regime through amendments to Australia's key piece of competition legislation, the Competition and Consumer Act 2010 (Cth).

At its core, CDR allows a consumer to obtain certain data held about that consumer by a third party and require data to be given to accredited third parties for certain purposes. By requiring businesses to provide public access to information on specified products they have on offer it is also intended to improve consumers' ability to compare and switch between products and services as well as encouraging competition between service providers which could lead to better prices for customers and more innovative products and services. In this way, the CDR provides a mechanism for accessing a broader range of information within designated sectors than is provided for by APP 12 in the Privacy Act given it applies not only to data about individual consumers but also business consumers and related products.

It is currently intended that the big four banks - Westpac Banking Corporation, Australia and New Zealand Banking Group Limited, National Australia Bank and The Commonwealth Bank of Australia - will participate in a pilot of the CDR from July 1, 2019 to January 31, 2020. During the pilot the banks will share product data about credit and debit cards, deposit accounts and

transaction accounts, with consumers and FinTechs also invited to take part in pilot. A full public roll out in the banking sector is slated for February 1, 2020, with the energy and telecommunications sectors to follow thereafter, and then other sectors across the economy to be added to the CDR over time.

The CDR systems covers competition, consumer, privacy and confidentiality matters. As such, it will be regulated by both the Australian Competition and Consumer Commission as well as the Office of the Australian Information Commissioner.

DEFINITIONS

Definition of personal data

Personal data (referred to as 'personal information' in Australia) means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in material form or not.

Definition of sensitive personal data

Sensitive personal data (referred to as 'sensitive information' in Australia) means information or an opinion about:

- Racial or ethnic origin
- Political opinions
- Membership of a political association
- Religious beliefs or affiliations
- Philosophical beliefs
- Membership of a professional or trade association
- Membership of a trade union
- Sexual orientation or practices
- Criminal record that is also personal information
- Health information about an individual
- Genetic information about an individual that is not otherwise health information
- Biometric information that is to be used for the purpose of automated biometric identification or verification
- Biometric templates

NATIONAL DATA PROTECTION AUTHORITY

The Privacy Commissioner, under the Office of the Australian Information Commissioner (OAIC) is the national data protection regulator responsible for Privacy Act oversight.

REGISTRATION

There is no registration requirement in Australia for data controllers or data processing activities. Under the Privacy Act, organizations are not required to notify the Office of the Privacy Commissioner of any processing of personal information.

DATA PROTECTION OFFICERS

Organizations are not required to appoint a data protection officer. However, the Privacy Commissioner has issued guidance

recommending that organizations appoint a data protection officer as good practice.

COLLECTION & PROCESSING

Organizations may not collect personal information unless the information is reasonably necessary for one or more of its business functions or activities.

Under the Privacy Act, organizations must take reasonable steps to ensure that personal information collected is accurate and up-to-date.

At or before the time organizations collect personal information, or as soon as practicable afterwards, they must take reasonable steps to provide individuals with notice of:

- Organization identity and contact information
- Why it is collecting (or how it will use the) information about the individual
- To whom it might give the personal information
- Any law requiring the collection of personal information
- The main consequences (if any) for the individual if all or part of the information is not provided
- The fact that the organization's privacy policy contains information about how the individual may access and seek correction of their personal information, how they may make a complaint about a breach of the APPs and how the organization will deal with such complaint
- Whether the organization is likely to disclose their personal information to overseas recipients and, if so, the countries in which such recipients are likely to be located

Organizations usually comply with these notification requirements by including the above information in a privacy policy and requiring individuals to accept the terms of that privacy policy prior to collecting their personal information.

In practice, a major Privacy Act compliance issue often arises because organizations fail to recognize that the mandatory notice requirements outlined above also apply to any personal information collected from a third party. Organizations must provide individuals with required notice on receipt of personal information from a third party, though they did not collect personal information directly from the individual. Unlike Europe, Australian privacy law does not distinguish between 'data processors' and 'data controllers.'

Organizations must not use or disclose personal information about an individual unless one or more of the following applies:

- The personal information was collected for the primary purpose of such disclosure or a secondary purpose related to (and, in the case of sensitive information, directly related to) the primary purpose of collection and the individual would reasonably expect the organization to use or disclose the information for that secondary purpose.
- The individual consents.
- The information is not sensitive information and disclosure is for direct marketing and it is impracticable to seek the individual's consent and (among other things) the individual is told that they can opt out of receiving marketing from the organization.
- A 'permitted general situation' or 'permitted health situation' exists; for example, the entity has reason to suspect that unlawful activity relating to the entity's functions has been engaged in, or there is a serious threat to the health and safety of an individual or the public.
- It is required or authorized by law or on behalf of an enforcement agency.

In the case of use and disclosure for the purpose of direct marketing, organizations are required to ensure that:

- Each direct marketing communication provides a simple means by which the individual can opt out

- The individual has not previously requested to opt out of receiving direct marketing communications

The above direct marketing requirements apply to all forms of direct marketing. Additionally, specific commercial electronic messaging requirements are outlined below under the heading "Electronic Marketing."

The Privacy Act affords additional protections when processing involves sensitive information. Organizations are prohibited from collecting sensitive information from an individual unless certain limited requirements are met, including one or more of the following:

- The individual has consented to the collection and the collection of the sensitive information is reasonably necessary for one or more of the entity's functions or activities.
- Collection is required or authorized by law or a court/tribunal order.
- A 'permitted general situation' or 'permitted health situation' exists (for example, where the information is required to establish or defend a legal or equitable claim or there is a serious threat to the life or health of the individual or the public).
- The entity is an enforcement body and the collection is reasonably necessary for that entity's functions or activities.
- The entity is a nonprofit organization and the information relates to the activities of the organization and solely to the members of the organization (or to individuals who have regular contact with the organization relating to its activities).

Organizations must provide individuals with access to their personal information held by the organization upon an individual's request. Additionally, individuals have a right to correct inaccurate, out-of-date, and irrelevant personal information held by an organization. Under certain circumstances, the organization may limit the extent to which it provides an individual with access or correction rights, including in emergency situations, specified business imperatives, and law enforcement or other public interests.

Further, organizations must provide individuals with the option to not identify themselves, or use a pseudonym, when dealing with the organization, unless it is impractical to do so or the organization is required or authorized by law to deal with identified individuals.

TRANSFER

Unless certain limited exemptions under the Privacy Act apply, personal information may only be disclosed to an organization outside of Australia where the entity has taken reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the personal information. The disclosing / transferring entity will generally remain liable for any act(s) done or omissions by that overseas recipient that would, if done by the disclosing organization in Australia, constitute a breach of the APPs. However, this provision will not apply where any of the following apply:

- The organization reasonably believes that the recipient of the information is subject to a law or binding scheme which effectively provides for a level of protection that is at least substantially similar to the Privacy Act, including as to access to mechanisms by the individual to take action to enforce the protections of that law or binding scheme. There can be no reliance on contractual provisions requiring the overseas entity to comply with the APPs to avoid ongoing liability (although it is a step towards ensuring compliance with the 'reasonable steps' requirement).
- The individual consents to the transfer. However, under the Privacy Act the organization must, prior to receiving consent, expressly inform the individual that if he or she consents to the overseas disclosure of the information the organization will not be required to take reasonable steps to ensure the overseas recipient does not breach the APPs.
- A 'permitted general situation' applies.
- The disclosure is required or authorized by law or a court/tribunal order.

SECURITY

An organization must have appropriate security measures in place (*ie*, 'take reasonable steps') to protect any personal information it retains from misuse and loss and from unauthorized access, modification or disclosure. The Privacy Commissioner has issued a 32-page detailed guidance document on what it considers to be reasonable steps in the context of security of personal

information, which we recommend be reviewed and implemented. Depending on the organization, and how and by which government agency it is regulated, as noted above specific requirements or expectations may also exist and with which organizations should be familiar. An organization must also take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for the purpose(s) for which it was collected.

BREACH NOTIFICATION

Entities with obligations to comply with the APPs under the Privacy Act must comply with mandatory reporting requirements under the mandatory data breach notification regime. This regime commenced on February 22, 2018.

The mandatory data breach notification includes data breaches that relate to:

- Personal information
- Credit reporting information
- Credit eligibility information
- Tax file numbers

In summary, the regime requires organizations to notify the OAIC and affected individuals of "eligible data breaches" (in accordance with the required contents of a notice). Where it is not practicable to notify the affected individuals individually, an organization that has suffered an eligible data breach must make a public statement on its website containing the required contents of the notice.

An "eligible data breach" occurs when the following conditions are satisfied in relation to personal information, credit reporting information, credit eligibility information or tax file information:

- Both of the following conditions are satisfied:
    - There is unauthorized access to, or unauthorized disclosure of, the information
    - A reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to which the information relates
- The information is lost in circumstances where both of the following apply:
    - Unauthorized access to, or unauthorized disclosure of, the information is likely to occur
    - Assuming that unauthorized access or unauthorized access disclosure were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to which the information relates

While "serious" harm is not defined in the legislation, the OAIC has released guidance on how serious harm may be interpreted and assessed by organizations. There are a number of key criteria to examine when determining if "serious" harm is likely to result from a breach which should be assessed holistically and take into account: the kinds of information, sensitivity, security measures protecting the information, the nature of the harm (*ie*, physical, psychological, emotional, financial or reputational harm) and the kind(s) of person(s) who may obtain the information.

The regime also imposes obligations on organizations to assess whether an eligible data breach has occurred where the organization suspects (on reasonable grounds) that an eligible data breach has occurred, but that suspicion does not amount to reasonable grounds to believe that an eligible data breach has occurred. Importantly, the OAIC has released guidance indicating that such assessments must be undertaken by organizations within 30 days of any suspected data breach.

There are various exceptions to the requirement to notify affected individuals and/or the OAIC of a data breach notification including in instances where law enforcement related activities are being carried out or where there is a written declaration by the Privacy Commission.

The introduction of the regime has resulted in many organizations requiring detailed contractual obligations with third party suppliers in relation to cybersecurity and the protection of personal information of their customers / clients. Complimenting this

regime, the OAIC has also released several guidance notes relating to the regime which include topics such as the security of personal information, while these are not legally binding, they are considered industry best practice.

Further, organizations may have additional obligations to notify other regulators of data breaches in certain circumstances. By way of example, in late 2018 the Australian Prudential and Regulatory Authority (APRA) released a new cross-industry prudential standard: Prudential Standard CPS 234 Information Security (CPS 234) to strengthen APRA-regulated entities' resilience against information security incidents (including cyberattacks), and their ability to respond swiftly and effectively in the event of a breach. CPS 234 will apply to all APRA-regulated entities who are expected to meet the new requirements by July 1, 2019 subject to certain transition periods in the case of information assets managed by third parties. Among other things, CPS 234 will require entities to notify APRA within 72 hours 'after becoming aware' of an information security incident and no later than 10 business days after 'it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner'. APRA also expects to release a revised CPG 234 Management of Security Risk in Information Technology in the first half of 2019 to provide guidance on the implementation of CPS 234.

ENFORCEMENT

The Privacy Commissioner is responsible for the enforcement of the Privacy Act and will investigate an act or practice if the act or practice may be an interference with the privacy of an individual and a complaint about the act or practice has been made. Generally, the Privacy Commissioner prefers mediated outcomes between the complainant and the relevant organization. Importantly, where the Privacy Commissioner undertakes an investigation of a complaint which is not settled, it is required to ensure that the results of that investigation are publicly available. Currently, this is undertaken by disclosure through the OAIC website of the entire investigation report.

The Privacy Commissioner may also investigate any 'interferences with the privacy of an individual' (*ie*, any breaches of the APPs) on its own initiative (*ie*, where no complaint has been made) and the same remedies as below are available.

After investigating a complaint, the Privacy Commissioner may dismiss the complaint or find the complaint substantiated and make declarations that the organization rectify its conduct or that the organization redress any loss or damage suffered by the complainant (which can include non-pecuniary loss such as awards for stress and/or humiliation). Furthermore, fines of up to AU$420,000 for an individual and AU$2.1 million for corporations may be requested by the Privacy Commissioner and imposed by the Courts for serious or repeated interferences with the privacy of individuals.

ELECTRONIC MARKETING

The sending of electronic marketing (which is referred to as 'commercial electronic messages' in Australia) is regulated under SPAM Act 2003 (Cth) ('SPAM Act') and enforced by the Australian Communications and Media Authority.

Under the SPAM Act a commercial electronic message must not be sent without the prior opt-in consent of the recipient.

In addition, each electronic message (which the recipient has consented to receive) must contain a functional unsubscribe facility to enable the recipient to opt out of receiving future electronic marketing.

A failure to comply with the SPAM Act (including unsubscribing a recipient that uses the unsubscribe facility) may have costly consequences, with repeat offenders facing penalties of up to AU$2.1 million per day.

ONLINE PRIVACY

There are no laws or regulations in Australia specifically relating to online privacy, beyond the application of the Privacy Act and State and Territory privacy laws relating to online / e-privacy, the collection of location and traffic data, or the use of cookies (or any similar technologies). If the cookies or other similar technologies collect personal information of a user the organization must comply with the Privacy Act in respect of collection, use, disclosure and storage of such personal information. App developers must also ensure that the collection of customers' personal information complies with the Privacy Act and the Privacy Commissioner has released detailed guidance on this.

KEY CONTACTS

Nicholas Boyle
Partner
T +61 2 9286 8479
nicholas.boyle@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

AUSTRIA

Last modified 10 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

In Austria, the laws concerning the implementation of the GDPR have been adopted gradually. In summer 2017, the existing Data Protection Act 2000 (*Datenschutzgesetz 2000*) was amended by the Data Protection Amendment Act 2018 (*Datenschutz-Anpassungsgesetz 2018*) which constituted the first implementation of various regulations related to GDPR, and was intended to enter into force simultaneously with GDPR. The 'Data Protection Act' (*Datenschutzgesetz, DSG)* has considerably amended the Data Protection Act 2000. In addition to the GDPR, it is now the central piece of legislation in Austria regulating data privacy.

The Privacy Deregulation Act 2018 (*Datenschutz-Deregulierungs-Gesetz 2018*) further amended the DSG. The DSG, as amended by the Privacy Deregulation Act 2018, came into force on May 25, 2018 and is now the applicable regulation in Austria. The DSG also includes the implementation of the Directive (EU) 2016/680.

In addition to the DSG, further amendments to other statutory laws were adopted in order to implement the GDPR (mostly to adapt to the terminology of the GDPR). These amendments were included in the General Data Protection Adjustment Act (*Materien-Datenschutz-Anpassungsgesetz 2018*) and the research-sector specific Data Protection Adjustment Act – Science and Research (*Datenschutz- Anpassungsgesetz 2018 – Wissenschaft und Forschung – WFDSAG 2018*). Further amendments in other laws have been made by the Second General Data Protection Adjustment Act, which

was passed in June 2018 and applies retroactively. Finally, ordinances were also passed regulating respectively the cases where a data privacy impact assessment is obligatory (the Obligatory DPIA Ordinance - *DSFA-V*) and the exemptions from the obligation to conduct a data privacy impact assessment (the DPIA Exemptions Ordinance - DSFA-AV).

Territorial Scope

As concerns the territorial scope of application, the relevant provisions of the (old) DSG 2000 have not been amended yet, and apply under the DSG as well. Thereunder, the DSG applies to processing of personal data in Austria, as well as processing of personal data in another EU Member State, if such processing occurs for the purpose of an Austrian-based main establishment or a branch office of a data controller. If, however, data are processed in Austria by a data controller organized under civil law which is based in another EU Member State, and the processing does not occur for the purposes of a branch office of such controller in Austria, the DSG stipulates that the laws of the state where the controller is based apply.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The DSG does not include any additional definitions or derogations as compared to the GDPR. However, Section 1 DSG, which provides a general basic (human) right to data privacy, does not use the definition of "data subject" of the GDPR, but rather uses the term "everyone" which is currently interpreted to include legal entities and other organizations too. Consequently, the basic (human) right to data privacy, as well as some basic data subject rights, as regulated in Section 1 DSG, also apply to legal entities and other organizations.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,*

processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Austrian Data Protection Authority (*Österreichische Datenschutzbehörde*) can be contacted at the following address:

Österreichische Datenschutzbehörde
Wickenburggasse 8
1080 Vienna
Austria / Europe
Phone number: +43 1 52 152-0
E-Mail: dsb@dsb.gv.at

If possible, the Austrian Data Protection Authority prefers to communicate via email.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The DSG contains in its Section 5 some additional regulation in respect to the rights and obligations of the data protection officer. Thereunder, the data protection officer and all persons working for the data protection officer are obliged to retain confidentiality regarding the identity of the persons that have approached the data protection officer as well as regarding all the circumstances that could reveal the identity of such persons.

The data protection officer and his assistant personnel have the statutory right to remain silent regarding the data obtained in their capacity as data protection officer, if a person employed in a position subject to the data protection officer's supervision is entitled to such right and to the extent that person has exercised such right. All files and other documents of the data protection officer which are subject to this statutory right to remain silent in the aforementioned extent cannot be lawfully seized.

Further regulations in Section 5 concern the data protection officers of public organizations.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the

controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Austrian DSG imposes further obligations upon controllers and processors. Pursuant to Section 6, all employees, agents or contractors of a controller or a processor who have access to personal data must be contractually obliged to transfer personal data only after receiving an adequate and documented instruction by their employer (confidentiality obligation). All employees, agents or contractors of a controller or a processor must be subject to confidentiality undertakings or professional or statutory obligations of confidentiality. Measures must be taken to ensure that all employees, agents or contractors of a controller or a processor are bound by the aforementioned undertakings and/or

obligations of confidentiality even after the termination of their respective contract, regardless of the cause or form thereof.

CCTV, or rather more broadly processing of images made in public or private spaces, including related sound recordings, are subject to further regulation and requirements pursuant to Sections 12 and 13 DSG. This provision provides limitations regarding the lawfulness of such processing as compared to Art 6 GDPR, as processing of image data is only permissible in the following cases:

- processing is necessary in order to protect the vital interests of the data subject
- the data subject has given their consent
- the processing is required or permitted by specific statutory law, or
- the interests of the data controller override the interests of the data subjects in the specific case, and the processing is proportionate

Overriding legitimate interests are assumed by the law in some cases listed as examples, such as preventive protection of property or persons on private properties or publicly accessible spaces controller by the data controller.

The capturing of images / CCTV is always prohibited in the following cases:

- processing of images capturing persons in their personal area of life without their express consent
- processing of CCTV images for the purpose of employee monitoring
- the automated comparison of personal data obtained by means of capturing images / CCTV without explicit consent and for the creation of personality profiles with other personal data, or
- the evaluation of personal data obtained by means of image capturing on the basis of special categories of personal data (Art. 9 GDPR) as a selection criterion

Other additional regulations for processing of data include:

- regulation relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Section 7), which allows processing of such data if they are publicly accessible, have been collected lawfully for other research purposes or other lawful purposes, or are pseudonymized; other data may only be processed to the extent there are specific statutory regulations, the data subjects have given their consent or the Data Protection Authority has approved the processing
- further regulation regarding the processing of data for purposes pursuant to Art 89(1) GDPR, most notably for research purposes, included in the Act on Research Organisation (*Forschungsorganisationsgesetz* - FOG); this regulation includes provisions which lessen to some extent the requirements for processing of special categories of data, including in particular the concept of "broad consent", and limit the rights of data subjects in this respect
- regulation relating to the processing of addresses for informing or sending questionnaires to data subjects (Section 8), which in principle requires consent for such processing, but also provides some derogations
- regulation regarding data processing in cases of catastrophes (Section 10)

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield

Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

Section 13 DSG imposes further obligations on Controllers in regard to CCTV and / or processing of captured images pursuant to Section 12 DSG. The controller needs to secure the access to the CCTV / captured images in a way that makes any access and / or subsequent alteration of captured images by an unauthorized third party impossible.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as

any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The Austrian Data Protection Authority is responsible for the enforcement of the GDPR. Pursuant to Section 11 DSG, the Austrian Data Protection Authority is obliged to impose administrative fines pursuant to the Article 83 GDPR in an adequate way. The Authority should in particular also apply the measures pursuant to Art 58 GDPR in case of first time breaches, in particular the possibility to issue warnings instead of imposing fines.

The fines under the GDPR shall be imposed under Austrian administrative criminal law. The Austrian administrative criminal law in general does not allow authorities to impose fines against a legal entity, but provides only for the liability of natural persons; in cases where violations are committed by a legal entity, the liable persons are either statutory representatives (directors) or persons appointed as responsible persons for adherence with specific administrative laws. However, the DSG provides a possibility to impose fines against legal entities, in the following cases:

- A violation of GDPR or DSG is committed by a natural person who has power (1) to represent the legal entity or to make decisions on behalf of the legal entity; or (2) has supervisory powers in the legal entity and has committed this offence either alone or as a part of an organ of the legal entity (*eg,* management board)

- An employee of the legal entity violates the provisions of GDPR or DSG and the violation was possible due to insufficient supervision or control by a person by a natural person that has power to (1) represent the legal entity; (2) or to make decisions on the behalf of the legal entity; or (3) has supervisory powers in the legal entity, provided the violation is not subject to criminal law.

The possibility to impose fines against legal entities is subject to the discretion of the Data Protection Authority, *ie,* the Authority may decide to impose fines against the legal entity or the responsible natural person, as appropriate. If the fine is imposed against the legal entity, the responsible natural person may not be fined for the same breach.

Public bodies cannot be fined for violations of GDPR or DSG.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg,* an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Act does not specifically address (electronic) marketing, while the use of personal data for marketing purposes clearly falls within the remit of the Act. It is arguable that the processing of personal data within the scope of the business is permissible for marketing purposes. However, it is argued that the consent of the data subjects is required.

Electronic marketing is also regulated by the Austrian Telecommunications Act (*Telekommunikationsgesetz* 2003, 'TKG'). Pursuant to the TKG the sending of electronic messages without prior consent of the recipient is unlawful, if the sending is for direct marketing purposes or to more than 50 recipients. No consent is required if the data has been obtained in the course of the sale of goods or provision of services, occurs for the same or similar goods or services, the recipient is able to decline easily and with no costs for the use of his or her personal data and the recipient has not previously declared, by requesting to be entered on to the relevant list (maintained by the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR)), that he or she does not want to be contacted.

The GDPR implementation acts do not provide any amendments or derogations in respect of electronic marketing. However, electronic marketing was and still is separately regulated in Austria in the Telecommunications Act (*Telekommunikationsgesetz 2003, TKG*), Section 107, which implements the ePrivacy Directive.

Pursuant to the TKG the sending of electronic messages without prior consent of the recipient is unlawful insofar as the message is sent for direct marketing purposes or to more than 50 recipients. Explicit consent is not required where (1) the data have been obtained in the context of the sale of goods or provision of services; (2) the electronic marketing concerns same or similar goods or services of the sender; (3), the recipient is able to decline easily and with no costs for the use of his or her personal data for electronic marketing, both when the data are collected as well as with each message received ('opt-out'), and the recipient has not previously declared, by requesting to be entered on to the relevant lists (the "Robinson lists", maintained by the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) and the Austrian Chamber of Commerce (WKO)), that he or she does not want to be contacted.

ONLINE PRIVACY

Online privacy is specifically regulated by the TKG.

Traffic Data

Traffic Data held by communications services providers (CSPs) must be erased or anonymized when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained for purposes of invoicing the services. In such a case, if the invoice has been paid and no appeal has been lodged with the CSP within three months the Traffic Data must be erased or anonymized.

Location Data

Location Data may only be processed for value added services and with consent of the user. Even in case of consent, the user must be able to prohibit the processing by simple means, for free of charge and for a certain time period.

Cookie Compliance

The relevant section of the TKG stipulates that a user must give informed consent for the storage of personal data, which includes a cookie. The user has to be aware of the fact that consent for the storage or processing of personal data is given, as well as the details of the data to be stored or processed, and has to agree actively. Therefore obtaining consent via some form of pop-up or click through agreement seems advisable. Consent by way of browser settings, or a pre-selected checkbox etc. is probably not sufficient in this respect.

If for technical reasons the short term storage of content data is necessary, such data must be deleted immediately thereafter.

Online privacy is still specifically regulated by the TKG, and the GDPR implementation acts have introduced only minor amendments thereto. There are no regulations regarding online privacy in the DSG itself.

Traffic Data

Traffic Data held by communications services providers ('CSPs') must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication. However, traffic data can be retained for the purpose of invoicing the services. In such a case, if the invoice has been paid and no appeal has been lodged with the CSP the traffic data must be erased or anonymised within three months.

Location Data

Location Data may only be processed for value added services and with consent of the user. Even in case of consent, the user must be able to prohibit the processing by simple means, for free of charge and for a certain time period.

Cookie Compliance

The relevant section of the TKG stipulates that a user must give informed consent for the storage of personal data, including cookies. The user shall be informed of the storage or processing of his / her data and shall explicitly consent to such storage or processing. Consent can for example be obtained via a pop-up or click through agreement. However, consent provided by way of browser settings, or a pre-selected checkbox etc. is not sufficient in this respect.

If it is necessary to store data for a short time period for technical reasons, such data must be deleted immediately thereafter.

KEY CONTACTS

Sabine Fehringer
Partner
T +43 1 531 78 1460
sabine.fehringer@dlapiper.com

Stefan Panic
Associate
T +43 531 78 1034
stefan.panic@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BAHRAIN

Last modified 28 January 2019

LAW

Bahrain enacted Law No. 30 of 2018 with respect to Personal Data Protection (Data Protection Law) on July 12, 2018. The Data Protection Law will be the main data protection regulation in Bahrain when it goes into force on August 1, 2019, and will supersede any law with contradictory provisions.

Notwithstanding the foregoing, Bahrain has a number of laws with provisions relating to data protection, including:

- Constitution of Bahrain 2002, provides citizens with a right to privacy, including confidentiality relating to postal, telegraphic, telephone and electronic communications
- Amiri Decree No. 15 of 1976 with respect to the Penal Code, protects individuals' right to privacy with provisions allowing sanctions against those who disclose information without consent from the concerned person
- Legislative Decree No. 9 of 1984 with respect to Central Population Register, prohibits divulging demographic information and imposes sanctions against those who disclose information without the consent from the concerned person
- Legislative Decree No. 54 of 2018 with respect to Electronic Letters and Transactions, which will come into force on February 1, 2019, protects the confidentiality of electronic records
- Legislative Decree No. 48 of 2002 with respect to Telecommunications, prohibits divulging confidential information
- Decree No. 64 of 2006 with respect to the Central Bank of Bahrain and Financial Institutions Law, contains provisions relating to confidential information and disclosing such information
- Resolution No. 8 of 2009 with respect to Licensees to implement Lawful Access, protects the subscriber's right to privacy in the telecommunications services domain
- Consumer Protection Guidelines Reference No. CCA/1112/451 (December 29, 2011), contains provisions on consumer privacy relating to personal information and calling patterns
- Law No. 35 of 2012 with respect to Consumer Protection, protects consumer privacy to maintain personal information and keep it from being exploited for other purposes
- Law No. 36 of 2012 with respect to Labour Law in the Private Sector, provides a right to privacy for employee data
- Decree No. 16 of 2014 with respect to the Protection of Information and National Documents, covers the importance of information relating to national security
- The Resolution No. 3 of 2015 with respect to Bulk Messaging protects recipients from unsolicited and solicited messages

- Law No. 60 of 2014 with respect to Information Technology Crimes, mentions the penalties of unlawful taping, capturing or intercepting, by technical means, any non-public transmission of information devices data to, from or within an information technology system
- The Central Bank of Bahrain Rulebook contains provisions relating to customer confidentiality during outsourced services and activities

DEFINITIONS

Definition of personal data

Personal data is defined under the Data Protection Law as any information of any form related to an identifiable individual, or an individual who can be identified, directly or indirectly, particularly through their personal identification number, or one or more of their physical, physiological, intellectual, cultural or economic characteristics or social identity.

Definition of sensitive personal data

Sensitive personal data is a subset of personal data. It is personal data which reveals, directly or indirectly, the individual's race, ethnicity, political or philosophical views, religious beliefs, union affiliation, criminal record or any data related to their health or sexual life. Sensitive personal data requires more rigorous treatment by data controllers. Sensitive personal data requires more rigorous treatment by data controllers.

NATIONAL DATA PROTECTION AUTHORITY

Under the Data Protection Law, Bahrain will have a new data protection authority, known as the Personal Data Protection Authority (Authority). The Authority will have power to investigate violations of the Data Protection Law on its own, at the request of the responsible Minister, or in response to a complaint.

The Authority can issue orders to stop violations, including issuing emergency orders and fines. Civil compensation is also allowed for any individual who has incurred damage arising from the processing of their personal data by the data controller (often referred to as a "data controller" in other data protection laws), or violating the provisions of the Data Protection Law by a business's data protection officer (often referred to as a "data protection officer" in other data protection laws). Finally, the most concerning feature of this law for businesses is that the Data Protection Law carries criminal penalties for violations of certain provisions.

REGISTRATION

The Authority must create a register of data protection officers. To be accredited as a data protection officer, an individual must be registered in that register.

DATA PROTECTION OFFICERS

Data controllers may voluntarily appoint a data protection officer. The Authority's Board of Directors may also issue a decision requiring specific categories of data controllers to appoint data protection officers. However, in all instances, the data controller must notify the Authority of such an appointment within three days of its occurrence.

A data protection officer must help the data controller in exercising its rights and fulfilling its obligations prescribed under the Data Protection Law. The data protection officer also has a number of other roles, including liaising with the Authority, verifying that personal data is processed in accordance with the Data Protection Law, notifying the Authority of any violations of the Data Protection Law that the data protection supervisor becomes aware of and maintaining a register of processing operations that the data controller must notify the Authority about.

The Authority must create a register of data protection officers. To be accredited as a data protection officer, an individual must be registered in that register.

COLLECTION & PROCESSING

Processing is defined under the Data Protection Law as any operation or set of operations carried out on personal data by automated or non-automated means, such as collecting, recording, organizing, classifying in groups, storing, modifying, amending, retrieving, using or revealing such data by broadcasting, publishing, transmitting, making them available to others, integrating, blocking, deleting or destroying them.

Processing of personal data can only occur with the consent of the data subject, (also referred to as the data owner) unless the processing is necessary:

- To implement a contract to which the data subject is a part
- To take steps at the request of the data subject to conclude a contract
- To implement an obligation required by law, contrary to a contractual obligation or an order from a competent court
- To protect the vital interests of the data subject
- To exercise the legitimate interests of the data controller or any third party to whom the data is disclosed, unless this conflicts with the fundamental rights and freedoms of the data subject

Processing of sensitive personal data is also prohibited without the consent of the data subject, unless one of the exceptions in Article 5 of the Data Protection Law apply.

Data controllers are prohibited from processing the following personal data types without the prior written authorization of the Authority:

- Automatic processing of sensitive personal data of persons who cannot provide consent
- Automatic processing of biometric data
- Automatic processing of genetic data (except for treatment provided by physicians and specialists at a licensed medical establishment, where the treatment is necessary for purposes of preventative medicine or diagnostic medicine, or for the provision of treatment or healthcare)
- Automatic processing that entails the connection of personal data files that are in the possession of two or more data controllers that are processing personal data for different purposes
- Processing that consists of visual recording to be used for monitoring purposes

TRANSFER

Transfers of personal data out of Bahrain is prohibited unless the transfer is made to a country or region that provides sufficient protection to personal data. Those countries need to be listed by the Authority and published in the Official Gazette.

Data controllers can also transfer personal data to countries that are not determined to have sufficient protection of personal data where:

- The data subject has consented to the transfer
- The data is from a public register
- The transfer is necessary for:
    - Executing a contract between the data subject and data controller, or taking preceding steps at the data subject's request for the purpose of concluding the contract

- Executing or concluding a contract between the data controller and a third party for the benefit of the data subject
- Protecting the data subject's vital interests
- Fulfilling a non-contractual obligation imposed by law, or an order of the court, public prosecution, an investigating judge or military prosecution, or
- Preparing, executing or defending a legal claim

Transfers can also be made with the permission of the Authority, issued on a case-by-case basis, if it deems that the data will be sufficiently protected.

SECURITY

The Data Protection Law requires that data controllers apply technical and organizational measures capable of protecting the data against unintentional or unauthorized destruction, accidental loss, unauthorized alteration, disclosure or access, or any other form of processing.

The Data Protection Law requires that the Authority's Board of Directors issues a decision specifying the terms and conditions that the technical and organizational measures must satisfy. The decision may require specific activities by applying special security requirements when processing personal data.

Data controllers must also use data processors who will provide sufficient guarantees about applying the technical and organizational measures that must be adhered to when processing the data. Data controllers must also take reasonable steps to verify that data processors comply with these measures.

BREACH NOTIFICATION

The Data Protection Law contains a general requirement on the data protection officer to notify the Authority of any breach under the Data Protection Law of which that the data protection officer becomes aware.

Mandatory breach notification

Under the Data Protection Law, there is no mandatory data breach notification provision requiring data controllers to notify the Authority or data subject in the event that there is a breach of personal data held by the data controller.

ENFORCEMENT

The Authority can issue orders to stop violations, including emergency orders and fines. Civil compensation is also allowed for any individual who has incurred damage arising from the processing of their personal data by the data controller, or arising from the data protection officer's violation of the Data Protection Law. Appeals can be made against decisions of the Authority.

The Data Protection Law also carries a range of criminal penalties and administrative fines for violating certain provisions.

Criminal penalties of imprisonment of not more than one year and / or a fine between BHD1,000 (US$2,645) to BHD20,000 (US$52,910), can be issued against any individual who:

- Processes sensitive personal data in violation of the Data Protection Law
- Transfers personal data outside Bahrain to a country or region in violation of the Data Protection Law
- Processes personal data without notifying the Authority
- Fails to notify the Authority of any change made to the data of which they have notified the Authority
- Processes certain personal data without prior authorization from the Authority

- Submits to the Authority or the data subject false or misleading data to the contrary of what is established in the records, data or documents available at their disposal
- Withholds from the Authority any data, information, records or documents which they should provide to the Authority or enable it to review them in order to perform its missions specified under the Data Protection Law
- Causes to hinder or suspend the work of the Authority's inspectors or any investigation which the Authority is going to make
- Discloses any data or information which he is allowed to have access to due to his job or which he used for his own benefit or for the benefit of others unreasonably and in violation of the provisions of the Data Protection Law

ELECTRONIC MARKETING

Under the Data Protection Law, data controllers must notify the data subject when data is collected directly or indirectly of whether data will be used for direct marketing purposes. Notice is important because it alerts data subjects of their right to object to any direct marketing relating to their personal data.

ONLINE PRIVACY

There is no specific online privacy regulation in Bahrain.

KEY CONTACTS

Mohamed Toorani
Legal Director - Head of Bahrain Office
T +973 1 755 0896
mohamed.toorani@dlapiper.com

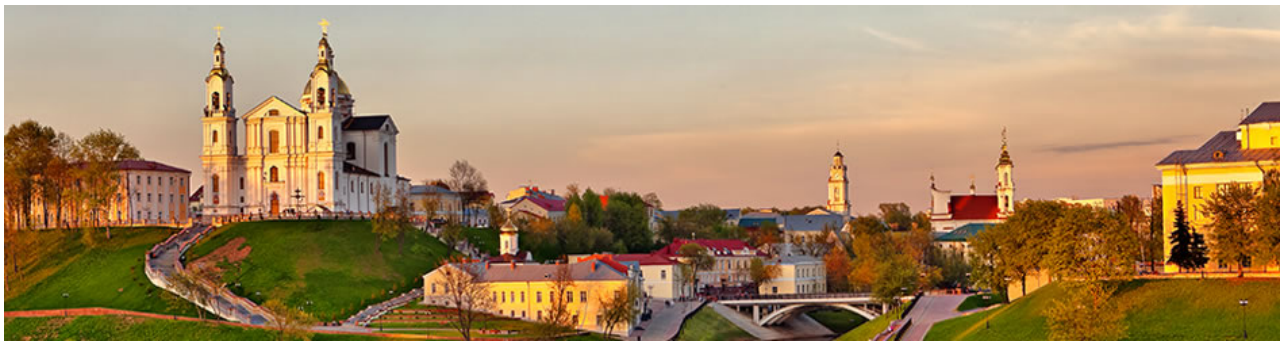
Noor Buhusayen
Legal Consultant
T +973 1 755 0893
noor.buhusayen@dlapiper.com

Lulwa Alzain
Trainee Legal Consultant
T +973 1 755 0891
lulwa.alzain@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BELARUS



Last modified 28 January 2019

LAW

The main legal acts regulating personal data protection in Belarus are the Law on Information, Informatisation and Information Protection of November 10, 2008 No. 455-Z (Information Protection Law) and the Law on Population Register of July 21, 2008 No. 418-Z (Population Register Law).

We expect adoption of the Law on Personal Data in 2019. It will be the first Belarusian legal act intended specifically for regulation of personal data protection issues. The draft Law on Personal Data was prepared and in July 2018 published for public discussions.

The acts implemented within the framework of the Eurasian Economic Union (EEU) should also be taken into consideration, *eg*, the Protocol on Informational Communication Technologies and Informational Interaction within the Eurasian Economic Union, Annex 3 to the Treaty on the Eurasian Economic Union of May 29, 2014. Following the Decision of the Supreme Eurasian Economic Council of October 11, 2017 the member states of EEU are planning to develop the initiative on conclusion of the Agreement on Data Circulation within the Union (including on personal data protection). The initiative is one of measures aimed at implementation of the Main Directions for Implementation of the Digital Agenda of the Eurasian Economic Union until 2025.

DEFINITIONS

Definition of personal data

According to the Information Protection Law, personal data consist of basic and additional personal data of an individual that are included in the population register, as well as other data enabling identification of certain individual. According to the Population Register Law basic personal data include the following types of information:

- Personal ID-number
- Name, second name, surname
- Gender
- Date and place of birth
- Digital photo
- Citizenship
- Information regarding registration at the place of residence or stay
- Information regarding death or recognition of a person to be dead, untraceable, incapable or partially capable

The list of additional personal is also indicated in Population Register Law and includes, inter alia, data on:

- A spouse
- Children
- Relatives
- Higher education
- Military duty performance
- Tax obligations

Belarus law does not define the notion of "other data enabling identification of certain individual." Arguably, mobile telephone number, email address, IP-address identifier could be recognized as personal data subject to certain conditions. However, there are no unified understanding on this issue among Belarusian researchers, as well as no confirmations based on court practice.

Definition of sensitive personal data

There is currently no concept of sensitive personal data under Belarus law.

The draft Law on Personal Data (in case adopted in currently available version) will introduce the definition of "special personal data." Special personal data will include information about race, nationality, political, religious and other convictions, health and sexual activity; criminal conviction records; biometric and genetic personal data.

NATIONAL DATA PROTECTION AUTHORITY

There are two main authorities involved in overseeing personal data protection issues: Operational and Analytical Centre under the Aegis of the President of the Republic of Belarus (the "Centre") and the Ministry of Communications and Informatisation of the Republic of Belarus (the "Ministry").

Should the draft Law on Personal Data be adopted in currently available version, special data protection authority will be designated in accordance with its provisions.

REGISTRATION

Belarusian law does not require any special registration for an entity / person to collect and process personal data or registration of a private information system (*eg*, database) used for processing of personal data. State information systems shall be registered regardless whether any personal data are processed in it or not. According to the Information Protection Law state information systems are information systems created and / or acquired at the expense of state or local budgets, state off-budget funds, or by state legal entities. Described registration can be performed for private owned information systems voluntarily. Registration is performed by specially authorized by the Ministry organization – SERUE "Institute of Application Software Systems." One of the conditions for state registration of an information system is registration of all information resources included in such an information system.

DATA PROTECTION OFFICERS

State bodies and legal entities which process personal data shall establish special departments or appoint employees responsible to ensure information protection. As a general rule, respective departments or appointed employees are responsible to take required technical and cryptography information protection measures. If for some reasons respective departments / employees cannot take such measures themselves, the head of a state body or a legal entity may involve a special organization licensed to perform activities on technical and / or cryptography information protection.

If the draft Law on Personal Data is adopted in its currently available version, a personal data operator which is a legal entity will be required thereunder to designate a special organizational unit (department, division, etc.) or appoint a person responsible of organization of collection, processing, distribution and provision of personal data.

COLLECTION & PROCESSING

Collection and processing of personal data must:

- Be performed only with a written consent of personal data subject
- Be performed in information systems equipped with information protection systems attested in the procedure established by the Centre (technical and cryptographic information protection means certified in accordance with Belarus law shall be used for creation of such information protection system)
- Be performed having implemented certain legal, organizational and technical measures for personal data protection

The legal measures may include concluding agreements with an individual whose personal data are collected and processed. Such agreements should stipulate the terms of personal data usage, as well as parties liability for breach of such terms.

The organizational measures may include establishing a special entrance regime to the premises used for collection and processing, designation of employees who can have an access to such premises and data, and differentiation of access levels to respective information.

The technical measures may include using cryptography, technical means and other possible measures of control over information protection.

TRANSFER

According to the Information Protection Law, transfer of personal data shall be carried out with written consent of the personal data subject. Currently there are no specific requirements established for transfer of personal data from Belarus to abroad.

In practice, the employers receiving the personal data of their employees carry out possible measures (legal, organizational, technical, etc.) to prevent illegal distribution of personal data and comply with Information Protection Law requirements.

Should the draft Law on Personal Data be adopted in currently available version, cross-border transfer of personal data will become specifically regulated. For example, transfer of personal data to countries not ensuring sufficient personal data protection measures will be permitted only in limited number of cases, including inter alia with an individual permit of data protection authority.

SECURITY

Appropriate technical, administrative and organizations security measures to secure personal data processed in an information system must be implemented.

BREACH NOTIFICATION

There are no general requirements under Belarusian law to report personal data protection breaches either to the state authorities, or the individuals whose personal data are concerned.

Certain requirements on notification of the Centre are set for specific cases of information protection system breach and inability to remove such breach within five working days.

Mandatory Breach Notification

There are no mandatory requirements under Belarusian law to report personal data protection breaches either to the state authorities, or the individuals whose personal data are concerned.

Certain requirements on notification of the Centre are set for specific cases of data protection system breach and inability to remove such breach within five working days.

Should the draft Law on Personal Data be adopted in its currently available version, it will establish obligation to notify data protection authority on breach of systems used for personal data protection immediately, but not later than within three days. This requirement will not cover minor breaches that could not lead to violation of the rights of personal data subject.

ENFORCEMENT

The key authorities involved in enforcement of the Law on Information Protection are the Ministry and the Centre.

Currently Belarusian law does not provide for any general liability for the breach of personal data protection requirements. Criminal and administrative liability can be applied for certain breaches related to data protection processing and violation of secrecy of person's private information.

For example, under the Criminal Code for intentional disclosure of adoption secrecy, a person could be sentenced to community works, criminal fine (as a general rule approximate amount of criminal fine is €300-10,000 (as of January 11, 2019)), or corrective works for the term up to one year; for unlawful collection or distribution of information regarding private life that is personal or family secrecy of another person without his / her consent (depending on certain circumstances), a person could be sentenced to community works, criminal fine, arrest, restriction or deprivation of liberty for up to three years.

As to examples of administrative sanctions, under the ode of Administrative Offenses for usage of information systems and data protection means not attested under applicable technical regulations (standards) in case attestation is obligatory a person / entity can be called to administrative fine with (or without) confiscation of the information protection means used. The approximate amount of fine in euro (as of January 11, 2019) is €50-200 – on a person, €100-200 – on an individual entrepreneur, €1000-2000 – on a legal entity.

ELECTRONIC MARKETING

Electronic marketing is subject to the rules established by the Law on Advertising of May 10, 2007 No. 225-Z (the "Advertising Law") and the Law on Mass Media of July 17, 2008 No. 427 Z (Mass Media Law).

According to the general rule of the Advertising Law names, pen-names, images or expressions of Belarusian citizens cannot be used in advertisements without their consent or consent of their authorized representatives. At the same time, advertisements about goods (work, services) offered by an individual entrepreneur shall contain information about his/her initials and surname.

Distribution of advertisements by telecommunication means (*eg*, telephone, telex, facsimile, mobile telephone communications, email) can be performed only with the consent of respective subscriber or addressee. The advertisement distributor is obliged to immediately stop advertising to subscriber or addressee upon his/her demand.

Individuals whose rights have been violated as a result of creation and / or distribution of an advertisement are entitled to protect their rights in court proceedings.

According to the Law on Mass Media, information about person's personal life or audio, video records and photos of a person can be distributed in mass media as a general rule only with consent of such person or his / her authorized representative.

ONLINE PRIVACY

Belarusian law does not specifically regulate online privacy. General requirements on personal data protection are applicable.

Certain online privacy requirements can be established under the legislation. For example, personal data of a person, who is a domain name administrator, can be disclosed in online WHOIS service of Belarusian domain zone only with consent of such person. However, consent is not required if the domain name was registered in the name of an individual entrepreneur.

KEY CONTACTS

Sorainen
www.sorainen.com/

Kirill Laptev
Senior Associate
T +375 17306 2102
kirill.laptev@sorainen.com

Anna Kasko
Associate
T +375 17 306 2102
anna.kasko@sorainen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BELGIUM

Last modified 17 October 2018

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The GDPR has been integrated in Belgium through a few new laws. The **'Data Protection Act'** of July 30, 2018 provides for the implementation of the GDPR's provisions open to further definition, derogation or additional requirements. It also includes the transposition of the 2016/680 Directive regarding the processing of personal data in the criminal justice chain and the establishment of a Control body on police information (called 'COC'). Additionally, it regulates the authorities outside the scope of the EU law (including intelligence and security services).[1]

The Belgian Data Protection Authority, the successor of the Belgian Privacy Commission, was established by the Belgian Federal Chamber of Representatives by the Law of December 3, 2017 (**'DPA Act'**)[2]. Adaptions to sectoral laws relying on the previous Data Protection Act will likely follow.

1. See the law.
2. See the law.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Data Protection Act builds on the definitions contained in the GDPR and further clarifies some notions, such as the notion of 'government'[1]. It further adds the definitions of a '**trusted third party**', '**disclosure of personal data'** and '**distribution of personal data**' in the context of the research and statistical purposes exception. The Act also clarifies certain concepts such as 'processing in the substantial public interest'[2], the 'processing for journalistic purposes'[3] and introduces new concepts such as 'a joint database'[4].

---

1. Art. 5 Data Protection Act.
2. Article 8 para. 1 Data Protection Act.
3. Art. 24 para. 1 Data Protection Act.
4. Article 48 Data Protection Act.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Data Protection Act appoints three more regulatory authorities (COC[1], Committee I[2] and Committee P[3]) with varying data protection related competences next to the general Data Protection Authority.

1. Art. 231 Data Protection Act.
2. Art. 72 para. 2 °7 Data Protection Act.
3. Art. 26 °7, c) Data Protection Act.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

The registration of processing activities through a notification has been abolished. In the public sector the Data Protection Act subjects the controller of processing activities in the context of police services to an obligation to publish a protocol detailing the transfer to a government body or private body based on public interest and compliance with legal obligations. [1]

1. Art. 20 Data Protection Act.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the

DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

In addition to the GDPR, the Data Protection Act requests the appointment of a DPO depending on the impact of the processing activity namely the high risk it may entail according to article 35 of the GDPR when (i) a private law body processes personal data on behalf of the government or the government transfers personal data to this private law body in the context of police services[1] or (ii) the processing falls under the exception necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[2] Some government bodies regulated by the Data Protection Act are also required to appoint a DPO.[3]

---

1. Art. 21 Data Protection Act.
2. Art. 190 Data Protection Act.
3. The Center for Missing and Sexually Exploited Children (Child Focus) Art. 8 para. 3 Data Protection Act; Governments for prevention, examination, detection and prosecution of criminal facts or the execution of penalties including the protection against and prevention of hazards for public safety implementing Directive 2016/680 Art. 63 e.v. Data Protection Act; Information and security services bodies Art. 91 Data Protection Act; Bodies for security authorisations Art. 124 Data Protection Act; The coordination department on threat analysis Art. 157 Data Protection Act.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an

official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two

months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Data Protection Act adds only specificities to the general processing requirements. The age for consent of children in the context of the information society services is 13 year.[1] When processing genetic, biometric and health data, a controller needs to indicate who has access to these personal data, keep a list of the categories of people who have access to these data, which is to be kept at the disposal of the DPA, and ensure that these people are bound by a legal, statutory or contractual obligation of confidentiality.[2] The Act provides a list of who or when one can process criminal data by requiring an access management list and confidentiality duties, as described here above.[3]

Data subject rights

The Data Protection Act provides further exceptions to data subject's rights, including the right to be informed when personal data is received from authorities under special regimes[4] or when personal data is disclosed to these bodies.[5] The special regimes addressed in the Act also enumerate the somewhat more limited data subject rights (rectification and verification), whether or not based on previous legislation.[6]

The Act clarifies that data subject rights, including the right to information in judicial proceedings/decisions, will be accommodated in accordance with the Judicial Code and the Code on Criminal proceedings.[7]

---

1. Art. 7 Data Protection Act.
2. Art. 9 Data Protection Act.
3. Art. 10 Data Protection Act.
4. Art. 11, Art. 13 and Art. 14 Data Protection Act.
5. Art. 12 Data Protection Act.
6. Art. 36 e.v., Art. 79, Art. 105 (9), Art. 113, Art. 145, Art. 173 Data Protection Act.
7. Art.16 Data Protection Act.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU - U.S. Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or

g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

No general additional requirements relating to transfers are introduced by the Data Protection Act. Notification requirements regarding transfers were previously embedded in Protocol accords and Royal Decrees which execute the legislation and it is currently unclear if those are being reconsidered. The Data Protection Act only regulates the transfer of personal data under the special regimes, which in certain cases provides for less leeway for transfers.[1]

---

1. Art. 66-70, Art. 93-94, Art. 126-127, Art. 159-160 Data Protection Act.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The Data Protection Act inserts no general additional requirements in relation to security measures. In the context of archiving, scientific or historical research purposes or statistical purposes, the Act sets out the different anonymization or pseudonymization requirements.[1] Security measures are also detailed for each special regime but resemble the GDPR.[2]

---

1. Art. 198 e.v. Data Protection Act.
2. Information Security Services Art. 88-89 Data Protection Act, Bodies for security authorisations Art. 121-122 Data Protection Act, Coordination department on threat analysis Art. 154-155 Data Protection Act, Passenger Information Art.179-180 Data

Protection Act.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

No general additional requirements are inserted in the Data Protection Act relating to security measures. Data breach obligations are also detailed for each special regime, but they resemble those contained in the GDPR.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;

- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The Act can be enforced by the data subject or by the Data Protection Authority (DPA)[1]. Under the Data Protection Act, a body, organisation or non-profit organisation can represent the data subject upon its request when it:

- was founded in accordance with Belgian law
- has legal personality
- has statutory objectives of public interest
- has been active in the area of the protection of personal data for at least 3 years[2]

The claim for an injunction of the processing activity should be brought before the Court of First Instance[3] except when the personal data is processed in criminal investigations, but there is no single court territorially competent. The DPA can impose administrative fines under article 83 of the GDPR varying from 10.000 EUR to 4% of the global annual turnover[4], but the government and their appointees are exempted[5]. A supervisory authority can exercise corrective measures but only over certain governmental bodies enumerated in the article.[6]

Depending on the infringement and the infringer, the controller, processor, compentent government body or the appointee can be subjected to criminal sanctions between 800 EUR – 160.000 EUR and a publication of the judgement.[7]

The DPA consists of 6 different Committees. The **inspection committee** of the DPA enjoys the power to identify persons, interview persons, conduct written interrogations, conduct on-site investigations, consult information systems and copy the data they contain, consult information electronically, seize or seal goods or computer systems and demand the identification of the subscriber or the normal user of an electronic communication service or of the electronic means of communication used.[8] Additionally, the inspector-general and the inspectors of the inspection committee may order the temporary suspension, restriction or freezing of the data processing activities that are the subject of an investigation if this is necessary to avoid a serious, immediate and difficult to repair disadvantage.[9] They can also request further information.[10]

The **dispute committee** will *inter alia* follow-up on a complaint but also propose a settlement, formulate warnings and reprimands, order compliance with data subjects'requests to exercise their rights , order the suspension of cross-border data flows but can also impose periodic penalty payments or administrative fines.[11]

Specific Regulations According to Art. 85 to 87 and Art. 89 GDPR

The legislator has made use of the opportunity offered by the GDPR to provide exemptions or derogations from certain obligations when the processing is carried out for journalistic purposes and the purposes of academic, artistic or literary expression. The Act exempts the controller not only from respecting data subjects' rights but also obligations of the controller (eg notification in case of breaches, transfer requirements, etc) and the investigative powers of the DPA.[12]

The Act also introduces two regimes for the derogations relating to the processing for archiving, scientific or historical research purposes or statistical purposes:

- general safeguards requiring among others register, information[13], contractual[14] and security requirements, or
- compliance with a code of conduct[15]

The Act does not include other derogations relating to employment.

---

1. Art. 211 par.3 Data Protection Act.
2. Art. 220 par. 2Data Protection Act.
3. Art. 209 Data Protection Act.
4. Art. 101 DPA Act
5. Art. 221 par. 2 Data Protection Act.
6. Art. 221 par. 1 Data Protection Act.
7. Art. 222 e.v. Data Protection Act.
8. Art. 66 DPA Act.
9. Art.70 DPA Act.
10. Art. 76 DPA Act.
11. Art. 95 DPA.
12. Art. 24 Data Protection Act.
13. Art. 193 Data Protection Act.
14. Art. 194 Data Protection Act.
15. Art. 187 Data Protection Act.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon,

the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Act applies to most electronic marketing activities, as there is likely to be processing and use of personal data involved (e.g. an email address is likely to be 'personal data' for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to object to the processing of their personal data (i.e. a right to 'opt out') for direct marketing purposes.

Additionally, specific rules are set out in the Belgian e-commerce legislation (Book XII of the Code of Economic Law) regarding opt-in requirements:

- These rules apply to all 'electronic messages', such as emails and text messages (Short Message Systems or SMS). Other types of electronic communication such as instant messaging and chat may also fall within the scope of these rules depending on the specific context. This covers not only clear promotional messages, but also newsletters and similar communications. Indeed, any form of communication intended to directly or indirectly promote goods, services, the image of a company, organisation or person which/who exercises a commercial, industrial or workmanship activity or regulated profession falls within the scope of these rules.
- As a general principle, the prior, free, specific and informed consent of the recipient of the message must be obtained ('opt-in principle').
- Two exceptions apply to the opt-in principle. No prior, free, specific and informed consent is to be obtained if:
    - the electronic marketing message is sent to existing customers of the service provider, or
    - the electronic message is sent to legal persons (e.g. to a general email address such as info@company.com).

  These exceptions are subject to compliance with strict conditions.
- Furthermore, all electronic messages must contain a clear reference to the recipient's right to opt out, including means to exercise this right electronically.

Neither the Data protection Act or the Data Protection Authority Act include provisions on electronic marketing or online privacy.

ONLINE PRIVACY

Cookies

Article 5 (3) of the E-Privacy Directive has been implemented into Belgian Law by means of an amendment to article 129 of the Belgian Electronic Communication Act.

The use and storage of cookies and similar technologies requires:

- the provision of clear and comprehensive information, and
- consent of the website user.

Consent is not required for cookies that are:

- used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or
- strictly necessary for the provision of a service requested by the user.

In February 2015 the DPA issued a recommendation on the use of cookies with useful guidance relating to the information obligation, the consent requirement and the exemptions.

Location data

Article 123 of the Belgian Electronic Communication Act stipulates that mobile network operators may process location data of a subscriber or an end user only to the extent that the location data has been anonymised, or if the processing is carried out in the framework of the provision of a service regarding traffic or location data.

The processing of location data in the framework of a service regarding traffic or location data is subject to strict conditions set forth in article 123.

The processing of location data must in addition also comply with the general rules stipulated by the Data Protection Act.

Traffic data

In accordance with article 122 of the Belgian Electronic Communication Act, mobile network operators are required to delete or anonymise traffic data of their users and subscribers as soon as such data is no longer necessary for the transmission of the communication (subject to compliance with cooperation obligations with certain authorities).

Subject to compliance with specific information obligations and subject to specific restrictions, operators may process certain location data for the purposes of:

- invoicing and interconnection payments
- marketing of the operator's own electronic communication services or services with traffic or location data (subject to the subscriber's or end user's prior consent), and
- fraud detection

Neither the Data protection Act or the Data Protection Authority Act include provisions on electronic marketing or online privacy.

KEY CONTACTS

Prof. Patrick Van Eecke
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +32 2 500 1630
patrick.van.eecke@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BERMUDA

Last modified 30 January 2018

LAW

The Bermuda legislature passed a comprehensive legislative framework that specifically addresses issues of data protection in the form of the Personal Information Protection Act 2016 (PIPA). The principal provisions of PIPA are not yet in force but are expected to come into force in late 2018.

Apart from PIPA, Bermuda law recognizes a duty of confidentiality in certain circumstances under the common law.

DEFINITIONS

Definition of personal data

PIPA provides for a definition of "personal information" as meaning "any information about an identified or identifiable individual".

At common law, information is generally to be regarded as 'confidential' if it has a necessary quality of confidentiality and has been communicated or has become known in such circumstances as give rise to a reasonable expectation of confidence; for example if obtained in connection with certain professional relationships, if obtained by improper means, or if received from another party who is subject to a duty of confidentiality.

Definition of sensitive personal data

PIPA provides for a definition of "sensitive personal information" as meaning "any personal information relating to an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information".

NATIONAL DATA PROTECTION AUTHORITY

PIPA makes provision for the office of a Privacy Commissioner. Certain sections of PIPA dealing the Privacy Commissioner were brought into force on 2 December 2016 but a Privacy Commissioner has yet to be appointed.

REGISTRATION

There is no system of registration and none provided for in PIPA.

DATA PROTECTION OFFICERS

There is currently no requirement to appoint a data protection officer. Once PIPA is fully in force, organisations covered by the legislation will be required to appoint a "privacy officer" for the purposes of compliance with PIPA.

COLLECTION & PROCESSING

Once fully in force, PIPA will regulate the collection and processing of personal information and will apply to any individual, entity or public authority collecting, storing and using personal information in Bermuda either electronically or as part of a structured filing system. The use to which sensitive personal information can be put by an organisation is much more restrictive.

The common law, which will continue to apply in parallel with PIPA, will in certain cases consider it a breach of confidence to misuse or threaten to misuse confidential information. The concept of 'misuse' is a broad one, but will often include any unauthorised disclosure, examination, copying or taking of confidential information. The precise scope of the term however will depend largely on the specific circumstances, including the relevant relationship and the nature of the information.

TRANSFER

Once fully in force, PIPA will regulate the transfer of personal information to an overseas third party. The legislation provides that the Privacy Commissioner can designate jurisdictions as providing comparable protection to Bermuda law. In other cases, the organisation subject to PIPA will be required to employ contractual mechanisms, corporate codes of conduct or other means to ensure that the overseas third party provides comparable protection for the personal information.

SECURITY

Once fully in force, PIPA will make provision for the implementation of proportional security safeguards against risk including loss, unauthorised access, destruction, use, modification or disclosure. In addition, a person who misuses or divulges confidential information (deliberately or otherwise) may be liable at common law.

BREACH NOTIFICATION

Once fully in force, PIPA will require notification of a breach of security leading to the loss or unlawful destruction or unauthorised disclosure of, or access to, personal information which is likely to adversely affect an individual to (a) the individual concerned; and (b) the Privacy Commissioner.

ENFORCEMENT

Once fully in force, PIPA will make provision for investigations and inquiries by the Privacy Commissioner and for a range of remedial orders that may be imposed by the Commissioner. It also provides for a claim for compensation for financial loss or emotional distress for failure to comply with the legislation (subject to a reasonable care defence). In addition, PIPA makes provision for criminal offences and penalties (including imprisonment) for misuse of personal information. In addition, a breach of the common law duty of confidentiality may give rise to a claim for, among other things, damages and/or an injunction. These remedies are to be sought through, and enforced by, the Bermuda courts.

ELECTRONIC MARKETING

The Electronic Transactions Act 1999 provided that the Minister responsible for electronic commerce had the power to issue a standard to apply to intermediaries or e-commerce service providers and such a standard was issued by the Minister on 5 May 2000 and came into force on 3 July 2000 (Standard). The definition of "e-commerce service provider" is "a person who uses electronic means in providing goods, services or information" while an "intermediary" (with respect to an electronic record) means "a person who, on behalf of another person, sends, receives or stores that electronic record or provides other services with respect to that electronic record". The Standard set out certain "Safe Harbour Guidelines" which included certain privacy requirements and the prohibition on the sale or transfer of personal data or business records of customers to another person for the purposes of sending bulk, unsolicited electronic records.

ONLINE PRIVACY

Once fully in force, PIPA will make special provision based on parental consent for certain uses of personal information about a child under the age of 14. Subject to this, there are no specific restrictions addressing online privacy of confidential information

beyond those generally applicable to the use of confidential information.

KEY CONTACTS

Carey Olsen
www.careyolsen.com/http://

Michael Hanson
Managing Partner
Carey Olsen
T +1 441 542 4501
michael.hanson@careyolsen.com

Keith Robinson
Partner
Carey Olsen
T +1 441 542 4502
keith.robinson@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BOSNIA AND HERZEGOVINA

Last modified 28 January 2019

LAW

The Law on Protection of Personal Data ('Official Gazette of BIH', nos. 49/06, 76/11 and 89/11) (DP Law) is the governing law regulating data protection issues in Bosnia and Herzegovina (BiH). The DP Law came into force on July 4, 2006 and was amended on October 3, 2011.

DEFINITIONS

Definition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable natural person. Data subjects are natural persons whose identity can be determined or identified, directly or indirectly, in particular by reference to a personal identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

The DP Law defines sensitive personal data as any data relating to any of the following:

- Racial, national or ethnic origin
- Political opinion, party affiliation, or trade union affiliation
- Religious, philosophical or other belief
- Health
- Genetic code
- Sexual life
- Criminal convictions
- Biometric data

NATIONAL DATA PROTECTION AUTHORITY

The Personal Data Protection Agency (DPA) is the national data protection authority in BiH. The DPA is seated in

Dubrovaka 6
Sarajevo

www.azlp.gov.ba

REGISTRATION

Each data controller (defined as a person or legal entity which processes personal data) must provide the DPA with specific information on the database containing personal data ("Database") established and maintained by the controller. The DPA maintains a publicly available register of data controllers and Databases.

The Database's registration includes two phases:

- First, the controller must register as a data controller (this registration as a controller is to be performed only once).
- Second, the controller must report to the Database's establishment, which has to be done within 14 days.

Registration of the Database is made by submitting the application in the prescribed form to the DPA. The DPA form includes information regarding:

- Data controller
    - Name
    - Address of its registered seat
- The Database itself
    - Processing purpose
    - Legal ground for its establishment
    - Identification of exact processing activities
    - Types of processed data
    - Categories of data subjects, and
    - Transfer of data abroad

If there is a subsequent change in the registered data, for example changing initial processing activities, the change needs to be reported to the DPA within 14 days from the date the change occurred.

DATA PROTECTION OFFICERS

There is no statutory obligation that the entity which processes personal data has a data protection officer. The Rules on the Manner of Keeping and Special Measures of Personal Data Technical Protection (Official Gazette of BiH no. 67/09) (Rules) stipulate that a controller can have an administrator of the Database. Such administrator is a natural person authorized and responsible for managing the Database and ensuring privacy and protection of personal data processing, in particular regarding implementation of security measures, storage and protection of data.

COLLECTION & PROCESSING

Collection and processing of personal data is permissible if carried out pursuant to the data subject's consent and in compliance with the basic principles of personal data protection.

The form of the data subject's consent depends on the type of personal data collected and processed. While the collection and processing of sensitive personal data requires explicit written consent from the data subject, the consent for the collection and processing of personal data falling within a category of general personal data does not have to be in writing. However, at the request of the competent authority, the controller has to be able to prove, at any time, the existence of a data subject's consent

for processing of both personal and sensitive personal data. Therefore, having a written consent for collection of any personal data is advisable. When required, written consent must contain at minimum elements prescribed by the DP law.

Apart from the consent, there are also other conditions which must be met for the collection and processing to be regarded as legitimate, including:

- Processing must be done in a fair and lawful way
- The type and scope of processed data must be proportionate to the respective purpose
- Other principles regarding the legitimate reasons for personal data processing

The DP Law provides an exception when a data subject's personal data may be processed without the data subject's consent. This is the case where the processing is necessary for the fulfillment of a data controller's statutory obligations or for preparation or realization of an agreement concluded between a data controller and a data subject (Exceptional Cases). These conditions are considered the basic principles of personal data protection and are applicable to each case of personal data processing.

TRANSFER

Under the transfer rules set out in the DP Law, processed personal data may be transferred to countries where an adequate level of personal data protection is ensured. In that regard, preferential status is given to the member states of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention"), as members of the Convention ensure an adequate level of personal data protection.

Personal data transfer to countries that do not provide for an adequate level of personal data protection is allowed in certain cases stipulated by the DP Law, for example:

- When the data subject consented to the transfer and was made aware of possible consequences of such transfer
- When it is required for the purpose of fulfilling the contract or legal claim
- When it is required for the protection of public interest

In addition, the DPA may exceptionally approve the transfer to a country that does not ensure adequate an level of personal data protection if the controller in the country where the data is to be transferred can provide for sufficient guarantees in regard to the protection of privacy and fundamental rights and freedoms of the data subject.

SECURITY

The DP Law requires data controllers and processors to:

- Take care of data security and to undertake all technical and organizational measures
- Undertake measures against unauthorized or accidental access to personal data, their alteration, destruction or loss, unauthorized transfer, other forms of illegal data processing, as well as measures against misuse of personal data
- Adopt a personal data security plan ("Security Plan") which specifies technical and organizational measures for the security of personal data

As provided by the Rules (as defined in the section "Data Protection Officers"), the Security Plan includes the categories of processed data and the list of instruments for protection of the data to ensure confidentiality, integrity, availability, authenticity, possibility of revision and transparency of the personal data.

The Rules prescribe that the controller is required to undertake more stringent technical and organizational measures when processing sensitive personal data. Such measures aim at enabling recognition of each authorized access to the information system, operation with the data during the controller's regular working hours and cryptographic protection of the data transmission via telecommunications systems with appropriate software and technical measures.

The Rules also closely regulate the manner of personal data keeping and personal data protection in automatic processing.

BREACH NOTIFICATION

The DP Law does not impose data security breach notification duty on the controller. However, the Rules do impose a duty on the Database's administrator, processor and performer to inform the controller on any attempt of unauthorized access to information system for the Database's management.

However, the regulations issued by the Communication Regulatory Agency (RAK) should be considered. The Regulation on Carrying out the Activities of the Publicly Available Electronic Communication Networks ('Official Gazette of BiH' no. 66/12) (Regulation A) stipulates that the operator of publicly available electronic communication networks (Operator) is required to inform RAK about its activities, operations and other applicable information required for RAK's regulatory competences. Since RAK's Regulation on Conditions for Providing the Telecommunications Services and Relation with End Users ('Official Gazette of BiH' no. 28/13) (Regulation B) prescribes for the Operator's obligation to undertake such methods which will protect the privacy of users and others, in a manner that will ensure the integrity and confidentiality of data, it can be concluded that the Operator is required to notify RAK of any breach of security and integrity of public telecommunication services that resulted in violation of protection of personal data or privacy of the respective services' s users.

When it comes to the notification duty towards the users, the Regulation B obliges the Operator to inform the users adequately (*eg*, in user agreement, in its terms and conditions or in the appropriate technical way) about the possibility of privacy or telecommunication facilities violations.

ENFORCEMENT

The DPA enforces the DP Law. The DPA is authorized and obliged to monitor implementation of the DP Law, both *ex officio*, and upon a third-party complaint. If the DPA finds that a particular person or entity processing personal data acted in violation of data processing rules, it may request that the controller discontinue such processing and order specific measures to be carried out without delay.

When acting upon the complaints, the DPA may also issue a decision by which it can order blocking, erasing or destroying of data, adjustment or amendment of data, temporary or permanent ban of processing, issue warning or reprimand to the controller. The decision of the DPA may not be appealed; however, a party may initiate administrative dispute before the Court of BiH.

The DPA can initiate a misdemeanor proceeding against the respective data controller before the competent court, depending on the gravity of the particular misconduct and the data controller's behavior with respect to the same. The offenses and sanctions are explicitly prescribed by the DP Law, which includes monetary fines for a controller in the amount between €2,550 and €51,100, as well as for the controller's authorized representative in the amount between €100 and €7,700.

Breach of personal data protection regulations represents a criminal offense of unauthorized collection of personal data by all criminal codes applicable in BiH (Criminal Code of BiH, Criminal Code of the Republic of *Srpska*, Criminal Code of the Federation of BiH and Crimes Code of *Brko Distrikt*). Prescribed sanctions are monetary fines (in amount to be determined by the court) or imprisonment up to six (6) months (Criminal Code of BiH; Criminal Code of the Federation of BiH; Criminal Code of the *Brko Distrikt*) or up to one (1) year (Criminal Code of the Republic of *Srpska*).

ELECTRONIC MARKETING

Although electronic marketing is not governed by the DP Law, the respective law regulates protection of personal data used in direct marketing. In that regard, the controller is not allowed to disclose personal data to a third party without the data subject's consent. However, when that is necessary for the protection of the controller's rights and interests and when it is not in contradiction with the data subject's right to the protection of personal privacy and personal life, the personal data may be used for direct marketing purposes without consent. The DPA is of the opinion that previous provision could be used only in explicit cases, when the controller is offering products or services to regular client in order to limit possible future damages for which he could be held responsible.

Under Regulation B, the Operator is prohibited from using user personal data for purposes of its business or other promotions,

unless it obtains explicit consent from the user to whom such data relates.

ONLINE PRIVACY

The general data protection rules, as introduced by the DP Law, are relevant for online privacy as well, as there are no specific regulations that explicitly govern online privacy. This includes obligation to act in accordance with the basic principles of personal data protection set out in the DP Law as well as acting on the basis of the data subject's informative consent.

KEY CONTACTS

Karanovic & Nikolic
www.karanovic-nikolic.com/

Nihad Sijercic
Attorney-at-law in cooperation with Karanovic & Nikolic
T +387 33 844 000
nihad.sijercic@karanovicpartners.com

Amina Dugum
Attorney-at-law in cooperation with Karanovic & Nikolic
T +387 33 844 000
amina.djugum@karanovicpartners.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BRAZIL

Last modified 28 January 2019

LAW

Brazil recently enacted the Brazilian General Data Protection Law (LGPD), Federal Law no. 13,709/2018, which was published on August 15, 2018. The LGPD is Brazil's first comprehensive data protection regulation and it is largely aligned to the EU General Data Protection Act (GDPR).

On December 28, 2018, the Provision Measure no. 869/2018 was published, which amended certain LGPD provisions and created the National Data Protection Authority (ANPD). Among other modifications, the LGPD will go into full force in August 2020, rather than February 2020 as required when the LGPD was first published. The LPGD, as amended, will take effect in August 2020.

Prior to the LGPD, data privacy regulations in Brazil consisted of various provisions spread across Brazilian legislation. For example, Federal Law no. 12,965/2014 and its regulating Decree no. 8,771/16 (together, the Brazilian Internet Act), which imposes some requirements regarding on security and the processing of personal data and other obligations on service providers, networks and applications providers, as well as rights of Internet users.

General provisions and principles applicable to data protection are also found in:

- The Federal Constitution
- The Brazilian Civil Code, and
- Laws and regulations that address
    - Particular types of relationships (*eg*, Consumer Protection Code [1] and employment laws)
    - Particular sectors (*eg*, financial institutions, health industry, or telecommunications), and
    - Particular professional activities (*eg*, medicine and law)

Additionally, there are laws on the treatment and safeguarding of documents and information handled by governmental entities and public bodies.

The LGPD applies to any processing operation carried out by a natural person or a legal entity, of public or private law, irrespective of the means used for the processing, the country in which its headquarter is located or the country where the data are located, provided that:

- The processing operation is carried out in Brazil
- The purpose of the processing activity is to offer or provide goods or services, or the processing of data of individuals located in Brazil, or
- The personal data was collected in Brazil

On the other hand, the law does not apply to the processing of personal data which is:

- Carried out by a natural person exclusively for private and non-economic purposes

- Performed for journalistic, artistic or academic purposes
- Carried out for purposes of public safety, national security and defense or activities of investigation and prosecution of criminal offenses (which will be the subject of a specific law), or
- Originated outside the Brazilian territory and are not the object of communication
- Shared data use with Brazilian processing agents or the object of international transfer of data with another country that is not the country of origin, provided that the country of origin offers a level of personal data protection adequate to that established in the Brazilian law

---

1. Due to a broad interpretation established in case law, practically every Internet user is considered a 'consumer' for consumer protection purposes.

DEFINITIONS

Definition of personal data

The LGPD defines **personal data** as any information related to an identified or identifiable natural person.

Anonymized data is not be considered personal data, except when the process of anonymization has been reversed or if it can be reversed applying reasonable efforts.

Definition of sensitive personal data

Sensitive personal data is defined as any personal data concerning:

- Racial or ethnic origin
- Religious belief
- Political opinion
- Trade union
- Religious, philosophical or political organization membership
- Health or sex life
- Genetic or biometric data

NATIONAL DATA PROTECTION AUTHORITY

The LGPD (as amended) established the National Data Protection Authority (ANPD), which will be composed of:

- A board of directors
- A national council (Council)
- An inspection body
- An ombudsman body
- Its own legal advisory body, and
- Administrative and specialized units for the enforcement of the LGPD

The ANPD will have the authority to issue sanctions for violations of LGPD. The Council of the ANPD has the authority to, among other things:

- Oversee the protection of personal data
- Issue regulations and procedures related to personal data protection
- Deliberate, at an administrative level, upon the interpretation of the LGPD and matters omitted in its redaction
- Supervise and apply sanctions in the event of data processing performed in violation of the legislation
- Implement simplified mechanisms for recording complaints about the processing of personal data in violation of the LGPD
- Request information, at any time, to controllers and processors of personal data that carry out processing operations of personal data

In addition, the ANPD Council will be responsible for, among other functions:

- Propose strategic guidelines for the creation of the National Policy for the Protection of Personal Data
- Suggest actions to be carried out by the ANPD
- Prepare studies and conduct public debates and hearings about the protection of personal data

REGISTRATION

There is currently no registration requirement before the National Authority under Brazilian law.

DATA PROTECTION OFFICERS

The LGPD creates the position of Chief of Data Treatment, which is the data protection officer (DPO) in charge for the data processing operation. The DPO will be responsible for the following:

- Accepting complaints and communications from data subjects and the National Authority
- Orienting employees about good practices and carrying out other duties as determined by the controller or set forth in complementary rules

The LGPD provides that the National Authority may further establish complementary rules about the definition and the duties of the DPO, including scenarios in which the appointment of such person may be waived, according to the nature and the size of the entity or the volume of data processing operations.

COLLECTION & PROCESSING

Under LGPD collection and processing is referred to as data treatment, and defined as all operations carried out with personal data, such as:

- Collection
- Production
- Reception
- Classification
- Utilization
- Access
- Reproduction
- Transmission
- Distribution
- Processing
- Filing
- Storage
- Elimination
- Evaluation
- Control
- Modification
- Communication
- Transfer
- Diffusion, or
- Extraction

The treatment of personal data may only be carried out based on one of the following legal bases, which largely align to the GDPR:

- With data subject consent
- To comply with a legal or regulatory obligation by the controller
- By the public administration, for the processing and shared use of data which are necessary for the execution of public

policies provided in laws or regulations or contracts, agreements or similar instruments
- For carrying out studies by research entities, ensuring, whenever possible, the anonymization of personal data
- For the execution of a contract or preliminary procedures related to a contract of which the data subject is a party
- For the regular exercise of rights in judicial, administrative or arbitration procedures
- As necessary for the protection of life or physical safety of the data subject or a third party
- For the protection of health, in a procedure carried out by health professionals or by health entities
- To fulfill the legitimate interests of the controller or a third party, and
- For the protection of credit

Notwithstanding the above, personal data processing shall be done in good faith and based on the following principles:

- Purpose
- Suitability
- Necessity
- Free access
- Quality of the data
- Transparency
- Security
- Prevention
- Nondiscrimination, and
- Accountability

As for the processing of sensitive personal data, the treatment can only occur when the data subject or her or his legal representative consents specifically and in highlight, for specific purposes; or, without consent, under the following situations:

- As necessary for the controller's compliance with a legal or regulatory obligation
- Shared data processed as necessary for the execution of public policies provided in laws or regulations
- For studies carried out by a research entity
- For the regular exercise of rights, including in a contract or in a judicial, administrative and arbitration procedure
- Where necessary to for the protection of life or physical safety of the data subject or a third party
- The protection of health, carried out by health professionals or by health entities, or
- ensuring the prevention of fraud and the safety of the data subject

The controller and operator must keep records of the data treatment operations they carry out, mainly when the processing is based on a legitimate interest.

In this sense, the ANPD may determine that the controller must prepare an Impact Report on Protection of Personal Data, including sensitive data, referring to its data processing operations, pursuant to regulations, subject to commercial and industrial secrecy. The report must contain at least a description of the types of data collected, the methodology used for collection and for ensuring the security of the information, and the analysis of the controller regarding the adopted measures, safeguards and mechanisms of risk mitigation.

TRANSFER

The transfer of personal data to other jurisdictions is allowed only subject to compliance with the requirements of the LGPD. Also, prior consent is needed for such transfer, unless:

- The transfer is to countries or international organizations with an adequate level of protection of personal data
- There are adequate guarantees of compliance with the principles and rights of data subject provided by LGPD, in the form of
    - Specific contractual clauses for a given transfer
    - Standard contractual clauses
    - Global corporate norms, or
    - Regularly issued stamps, certificates and codes of conduct
- The transfer is necessary for international legal cooperation between public intelligence, investigative and prosecutorial

agencies
- The transfer is necessary to protect life or physical safety of the data subject or of third party
- Authorization has been provided by the ANPD
- The transfer is subject to a commitment undertaken through international cooperation
- The transfer is necessary for the execution of a public policy or legal attribution of public service
- The transfer is necessary for compliance with a legal or regulatory obligation, execution of a contract or preliminary procedures related to a contract, or the regular exercise of rights in judicial, administrative or arbitration procedures

SECURITY

Controllers and processors must adopt security, technical and administrative measures able to protect personal data from:

- Unauthorized accesses, and
- Accidental or unlawful situations of:
    - Destruction
    - Loss
    - Alteration
    - Communication, or
    - Any type of improper or unlawful processing

The LGPD grants the ANDP authority to establish minimum technical standards which are required to be implemented.

The Brazilian Internet Act further establishes that service providers, networks and applications providers should keep access records (such as IP addresses and logins) confidential, in a secured and controlled environment. Guidelines issued pursuant to the Internet Act established guidelines on appropriate security controls, including:

- Strict control on data access by defining the liability of persons who will have the possibility of access and exclusive access privileges to certain users
- Prospective of authentication mechanisms for records access, using, for example, dual authentication systems to ensure individualization of the controller records
- Creation of detailed inventory of access to connection records and access to applications containing the time, duration, the identity of the employee or the responsible person for the access designated by the company and the accessed file
- Use of records management techniques that ensure the inviolability of data, such as encryption or equivalent protective measures

BREACH NOTIFICATION

The controller must report to ANDP and the data subject in a reasonable time period (to be further defined by the ANDP), if the breach is likely to result in risk or harm to data subjects.

The notice must contain, at least, the following:

- Description of the nature of the affected personal data
- Information regarding the data subjects involved
- Indication of the security measures used
- The risks generated by the incident
- The reasons for delay of communication (if any)
- The measures that were or will be adopted

Additionally, the ANDP shall verify the seriousness of the incident and may, if necessary to safeguard the data subject's rights, order the controller to adopt measures, such as the broad disclosure of the event in communications media, as well as measures to reverse or mitigate the effects of the incident.

ENFORCEMENT

The LGPD provides for penalties in case of violations its provisions. Data processing agents that commit infractions can be subject to administrative sanctions, in a gradual, single or cumulative manner, including a fine, simple or daily, of up to 2% of the revenues of a private legal entity, group or conglomerate in Brazil, up to a total maximum of R$50 million per infraction.

Other sanctions can include:

- Warning
- Publicizing of the violation
- Blocking the personal data to which the infraction refers to until its regularization
- Deletion of the personal data to which the infraction refers to

Until the LGPD takes effect, the level of enforcement by the ANDP is uncertain. The controller or the processor which causes material, moral, individual or collective damage to others is liable to individuals for such damages, including through a class action.

Exceptions to the obligation to repair occurs only if:

- The agent (*ie*, controller or the processor) did not carry out the data processing
- There was no violation of the data protection legislation in the processing, or
- The damage arises due to exclusive fault of the data subject or a third party

ELECTRONIC MARKETING

The LGPD does not specifically address electronic marketing and Brazil has no other specific legislation in this regard.

Obtaining opt-in consent from consumers prior to sending marketing emails is recommended. However, according to 'Brazilian Code of Best Practice of Marketing E-mail', a soft opt-in is also possible in scenarios of prior and verifiable commercial or social relationship with the user. In this case, it will be being necessary to:

- Send the message by an email address linked to the company's domain name (where the company has a prior commercial relationship with the recipient)
- The subject of the message shall be related to its content, and
- Opt-out must be offered or available to user, preferably in the message

In spite of the lack of a specific statute, general provisions on privacy and intimacy rights, as well as consumer protection rights also apply to electronic marketing; thus, the sender should immediately cease sending any sort of electronic marketing if so requested by the consumer.

ONLINE PRIVACY

The Brazilian Internet Act has several provisions concerning the storage, use, disclosure and other treatment of data collected on the Internet. Also, the established rights of privacy, intimacy and consumer rights apply equally to electronic media, such as mobile devices and the Internet. So, violations of these rights may be subject to civil enforcement as well.

Furthermore, as explained in prior sections, identifiable data are also encompassed under the scope of protection of the LGPD. Thus, in case cookies and location data are associated with a natural person, their collection should also observe the same obligations provided by the Brazilian data protection law. The obligation doesn't apply, however, to anonymized data, which is not considered personal data under the LGPD unless the process of anonymization has been reversed or can be reversed applying reasonable efforts.

That said, consent to cookies is generally necessary where they involve the collection and handling of personal data from a user (*eg*, the information is linked or linkable a particular user, IP address, a device or other particular identifier) unless such collection and treatment can be justified under another legal basis set forth by the LGPD (please refer to the prior section on Collection and Processing).

KEY CONTACTS

Campos Mello Advogados
www.camposmello.adv.br/

Paula Mena Barreto
Partner
Campos Mello Advogados
T +55 21 3262 3028
paula.menabarreto@cmalaw.com

Manoela Quintas Esteves
Associate
Campos Mello Advogados
T +55 21 3262 3042
manoela.esteves@cmalaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BRITISH VIRGIN ISLANDS

Last modified 28 January 2019

LAW

The British Virgin Islands (BVI) has not enacted formal legislation to regulate data protection. However, it is expected that BVI will promulgate data protection legislation in the near future to adapt internationally recognized standards.

BVI accepts English common law as persuasive authority. BVI courts accordingly recognize the common law duties of privacy and confidentiality. Entities have a duty to maintain confidentiality in a person's details, unless an applicable exception applies. The duty of confidentiality has been statutorily codified in various aspects of BVI legislation, including the Banks and Trust Companies Act, 1990 (as amended), which regulates all banking, trust and fiduciary related activities in BVI.

The common law duty of privacy and confidentiality is limited by specific exceptions under applicable anti-money laundering legislation, primarily regulated under the BVI Proceeds of Criminal Conduct Act, 1997, and the Anti-Money Laundering Regulations, 2008.

DEFINITIONS

Definition of personal data

There is no specific definition of personal data.

Definition of sensitive personal data

There is no specific definition of sensitive personal data.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in the BVI. Instead, courts are guided by the English common law duties of privacy and confidentiality. The Financial Services Commission (Commission) regulates the fiduciary and trust business sectors pursuant to the Banks and Trusts Companies Act, 1990 (as amended).

REGISTRATION

There are no data protection registration requirements in the BVI.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer in the BVI.

COLLECTION & PROCESSING

Entities that manage and maintain personal data in the BVI are subject to the common law duties of privacy and confidentiality. Fiduciary and trust licensees are required to maintain the privacy and confidentiality of client personal data, and may not release or disseminate such information to third parties without specific permission from the individual. This obligation may be limited under applicable anti-money laundering legislation.

With respect to corporate data, the Registrar of Corporate Affairs (Registrar) is permitted to release limited information regarding registered companies, including company name, type, registration or incorporation date, registered office address and company status. Shareholder and director information is not publicly accessible unless specifically disseminated by company authorization, except where required by law to assist law enforcement agencies. Government officials, professional agents, attorneys and accountants, and their employees, are prohibited from disclosing information.

TRANSFER

The common law duty of privacy and confidentiality applies to third party data transfers. Depending on the nature of data, a statutory duty may apply where the common law duty of privacy and confidentiality has been codified. Entities should ensure that required consent is obtained prior to any third party data transfer.

The Computer Misuse and Cybercrime Act, 2014 regulates and penalizes the unauthorized transfer and dissemination of information stored on a computer.

The Commission retains a limited exception to the duty of privacy and confidentiality when disclosing information to certain third parties. For example, the Commission may disclose information to foreign regulators in approved jurisdictions to enable foreign regulators to exercise functions similar to that of the Commission. Prior to disclosure, the foreign regulator must certify that information will not be transmitted to any individual without prior written consent from the Commission.

SECURITY

There are no formal statutory security measures in place. Entities that maintain personal data are generally required to ensure technical and organizational safeguards are in place to protect the confidentiality of personal data and confidential information.

BREACH NOTIFICATION

There is no requirement to report data security breaches in the BVI.

ENFORCEMENT

The Commission and the BVI courts are responsible for enforcement of violations of the duty of privacy and confidentiality.

ELECTRONIC MARKETING

There is no formal electronic communications legislation in place. The Telecommunications Act (No 10 2006) regulates the BVI telecommunications industry and provides sanctions to protect the confidentiality of personal data.

ONLINE PRIVACY

There is no online privacy legislation in the BVI.

KEY CONTACTS

Carey Olsen
www.careyolsen.com

Alan Hughes
Senior Associate
T +1 284 494 4030
alan.hughes@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BULGARIA

Last modified 10 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

Bulgaria implemented the EU Data Protection Directive 95/46/EC with the Personal Data Protection Act (In Bulgarian:), promulgated in the State Gazette No. 1 of January 4, 2002, as amended periodically (Act). The Act came into force on January 1, 2002.

In view of the entry into force of Regulation (EU) 2016/679 (General Data Protection Regulation - 'GDPR'), on April 30, 2018 a draft law amending and supplementing the Personal Data Protection Act ('Draft Law') was introduced for public discussion. Public consultations ended on May 30, 2018 and the Draft Law was submitted to the Parliament where it is subject to further amendments.

The objectives of the Draft Law are to ensure the effective implementation of the GDPR and the fulfillment of the obligations of the Republic of Bulgaria as an EU Member State with respect to transposing into national legislation Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

The Draft Law complements the GDPR by providing regulation to matters in the field of personal data processing that

have not been explicitly covered by the GDPR, or where the GDPR has left room for the exercise of legislative discretion. As the regulation has direct effect and is applicable in all EU member-states without the need of adopting a designated legislative act, the Bulgarian legislator has adopted the approach of directly referring to and implementing the GDPR without repeating the core provisions of the regulation in the Draft Law.

The Draft Law designates the Commission for Personal Data Protection as the sole supervisor responsible for protecting the fundamental rights and freedoms of individuals with regard to the processing and free movement of personal data within the European Union. The Draft Law further regulates the legal remedies in cases of violation of personal data law, the accreditation and certification in the field of personal data protection, the administrative liability and the administrative measures in cases of violations of the Draft Law.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

Definition of personal data

The Draft Law repeals the definition of personal data as described in the current Personal Data Protection Act and explicitly refers to the definition of personal data under art. 4 of the GDPR (§1 of the Supplementary provisions of the Draft Law).

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of sensitive personal data

The Draft Law repeals the definition of sensitive data under the current Personal Data Protection Act and implies that the definition under the GDPR would apply following its direct effect in all EU member states.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Bulgarian data protection authority (DPA) is the Personal Data Protection Commission (In Bulgarian: , the 'Commission').

2 Professor Tsvetan Lazarov, Sofia 1592
Bulgaria
kzld@cpdp.bg
www.cpdp.bg

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

The Draft Law repeals the current requirement for registration of data controllers before the local DPA.
Pursuant the Draft Law the DPA shall maintain the following public registers:

- register of data controller and data processors who have appointed data protection officers;
- register of the accredited certifying bodies under art. 14;
- register of codes of conduct.

The DPA shall also support an internal register of established breaches of the GDPR and the Personal Data Protection Act, as well as a register of the measures taken in accordance with art. 58, para 2 of the GDPR, which however shall not be made public.

The rules for maintaining the registers, their content and access thereto shall be regulated in Rules of Procedure to be adopted by the DPA.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

There is no explicit requirement for a data protection officer set out by the Draft Law, thus the general requirement pursuant to the GDPR shall apply. Pursuant to the Draft Law, data controllers shall be further obliged to communicate the personal details and contact details of the DPO, as well as any subsequent replacements, before the local DPA, and will also have to publish their contact details. The form and content of the notification and the procedure before the local DPA shall be regulated in the Rules of Procedure of the Commission and its Administration to be adopted by the DPA.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");

- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or

c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Bulgarian Draft Law does not repeat the core provisions of the GDPR relating to collection and processing of personal data in its body, but directly refers to Art. 6, para (1) (legal grounds for processing) and Art. 5 (principles for data processing) GDPR (art. 25a of the Draft Law). In case the data subject provides his / her personal data to a data controller or a data processor in breach of these provisions, the data controller / data processor should have to immediately return the data or delete / destroy the data within one month of becoming aware of the breach.

The Draft Law also introduces additional rules relating to specific data processing situations:

- Conditions applicable to child's consent in relation to information society services - The Draft Law introduces a lower age of the data subject, under which the consent of a parent or a guardian would be required for the lawful processing of personal data of a child in cases of direct provision of information society services. Under the Draft Law if the data subject is under 14 years old, a consent by a parent exercising the parental rights or by guardian of the data subject is required for the lawful processing of the data.
- Processing of personal identification number - The Draft Law addresses a topic which was largely discussed by data subjects and data controllers – the personal identification number possessed by each Bulgarian citizen. Should the Draft Law be adopted, public access to personal identification number / personal identification number of a foreigner ('PIN/PINF') shall be granted only if required by law. The law should define the terms and conditions of granting such access, in order to prevent that the PIN/PINF is made publicly available, where 'public availability' means the disclosure of personal data or otherwise providing access to them to an unlimited number of persons without taking measures to ensure accountability. Data controllers providing electronic services should undertake appropriate technical and organizational measures to prevent the PIN/PINF from being the sole identifier for the use of their services.
- Processing and freedom of expression and information - Where personal is processed for the exercise of freedom of expression and information, including for journalistic purposes and for the purposes of academic, artistic or literary expression, the data controller should assess the lawfulness of such processing in each particular case. The assessment should be made based on a number of criteria, such as:

  the type of personal data; the impact the public disclosure of the personal data would have on the privacy of the data subject and his/her reputation; the circumstances under which the personal data have become known to the data controller; the character and nature of the statement by which the freedom of expression and information has been exercised; the importance of the disclosure of personal data for clarifying a matter of public interest; whether the data subject is a person who holds a position under the Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act or is a person who, due to the nature of his / her activity or role in public life, has a lesser degree of protection of his / her privacy or whose actions have an impact on society; whether the data subject has contributed to the disclosure of his / her personal data and / or information on his or her personal and family life; the purpose, content, form and consequences of the statement by which the freedom of expression and information has been exercised; the compliance of the statement by which the freedom of expression and information has been exercised, with the fundamental citizens rights; other circumstances relevant to the particular case.

The data controller's decision should not disproportionately restrict the freedom of expression and information.

- Processing in the context of employment - The Draft Law regulates explicitly certain matters related to personal data processing in the context of an employment relationship. The Draft Law provides that employers may copy employee's identification document, driving license or residence document only if required by law. The employers should adopt rules and procedures for:

the use of breach reporting system; restrictions on the use of internal company resources; introduction of systems for control access, working time and labor discipline.
These rules and procedures shall contain information on the scope, obligations and methods with respect to their application. The Draft Law recognizes that the business purpose of the employer and the nature of the related work processes shall have to be taken into account upon the adoption of the rules and procedures. The rules and procedures will have to be brought to the attention of the employees. Employers shall have to further determine a retention period for the personal data collected during the recruitment process, which however may not be longer than six months, unless the candidate consented to a longer period. Where the employer has, for recruitment purposes, requested original or notarized copies of documents certifying the physical and mental fitness of the applicant, the required degree, or the length of service for the previous positions occupied, the candidate data subject may request the return of the submitted documents within six months of the conclusion of the recruitment procedure and upon such request the employer should return the documents in the same form they were submitted.

- Personal data processing by way of large-scale surveillance of publicly accessible areas - Under the Draft Law data controllers and data processors shall adopt special rules for the processing of personal data through systematic large-scale surveillance of publicly accessible areas, including via video surveillance. The Draft Law provides a definition for 'large-scale' - a systematic monitoring and / or processing of personal data of an unlimited number of data subjects. The rules for personal data processing through large-scale surveillance of publicly accessible areas shall define the legal grounds and objectives for the introduction of a monitoring system, the location, scope and means of monitoring / surveillance , retention periods for the information records and their deletion, the right of review by the persons being surveilled, the means of informing the public about the monitoring carried out, as well as the restrictions on granting access to such information to third parties. The minimum requirements for data controllers / data processors with respect to the aforementioned obligations shall be published on the website of the DPA.

Processing of personal data of deceased persons

The Draft Law stipulates, that when processing the personal data of deceased persons data controllers shall have to take appropriate measures to prevent the rights and freedoms of others and the public interest from being adversely affected. In such cases, the data controller may retain the data only if there is a legal basis therefor. In addition, data controllers shall provide upon request access to the personal data of a deceased person, including a copy thereof, to his / her heirs or other persons with legal interest.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules, standard contractual clauses, and the EU - US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;

b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Draft Law does not derogate from the provisions of the GDPR regarding data transfer and does not introduce any additional rules or requirements in this respect. Following the direct effect of the GDPR in all EU member states, the provisions of the regulation relating to this matter shall be applied in all cases of data transfer.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The Draft Law does not derogate from the provisions of the GDPR regarding security of personal data and does not introduce any additional rules or requirements in this respect. After the entry into force of the GDPR the current DPA's regulation on the minimum level of technical and organizational measures, as well as the minimum required type of protection, has been repealed and is expected to be transformed into a Methodological Guidance.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority,

and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Draft Law does not derogate from the provisions of the GDPR regarding data breach notification and does not introduce any additional rules or requirements in this respect. Following the direct effect of the GDPR in all EU member states, the provisions of the regulation relating to this matter shall be observed.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide

turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The Draft Law designates the Commission as the overall supervision and control regarding compliance with the GDPR in Bulgaria. The Draft Law defines the competences of the Commission by referring to art. 57 and 58 of the GDPR. Apart from performing the powers under the GDPR, the DPA shall be entitled to:

1. analyze and carry out overall supervision and ensure compliance with the GDPR, the Draft Law and the legislative acts in the area of personal data protection;
2. issue secondary legislation in the area of personal data protection;
3. ensure the implementation of the decisions of the European Commission on the protection of personal data and the implementation of binding decisions of the European Data Protection Supervisor
4. participate in international cooperation between data protection authorities and international organizations on personal data protection issues;
5. participate in the negotiation and conclusion of bilateral or multilateral agreements on matters within its competence;
6. organize, coordinate and conduct training in the field of personal data protection;
7. issue administrative acts related to its authority in the cases provided for by law;
8. adopt criteria for the accreditation of certification bodies;
9. issue guidelines, recommendations and best practices in cases where such are not issued by the European Data Protection Supervisor.
10. bring proceedings before the court for breach of the GDPR;
11. issue mandatory instructions, give instructions and recommendations regarding the protection of personal data;
12. impose coercive administrative measures.

The Commission is also entitled to further clarify in its internal Rules of Procedure its tasks, procedures and rules for work of its administration, as well as rules for the proceedings before the Commission.

The Draft Law does not derogate from the provisions of the GDPR regarding administrative sanctions, but directly refers to the amounts of fines and pecuniary sanctions set out by the GDPR and the respective criteria for their determination. The Draft Law specifies that all sanctions shall be imposed in the BGN equivalent of the EUR amounts set by the GDPR.

For other violations under the Draft Law the data controller / data processor shall be subject to a fine or a pecuniary sanction of BGN 1000 up to BGN 5000;

The Commission's decisions are subject to appeal before the Administrative Court Sofia within 14 days of receipt. Decisions of the Administrative Court are subject to appeal before the Supreme Administrative Court which decisions are final.

In case of a violation of his / her rights under the GDPR and the Draft Law, every data subject is entitled to refer the matter to the DPA within one year of becoming aware of the breach, but no later than five years from the breach taking place. In addition, data subjects shall be entitled to appeal the actions and acts of the data controller / data processor directly before the administrative courts or the Supreme Administrative Court, except where there are pending proceedings before the Commission for the same matter if a decision regarding the same breach has been appealed and there is not yet a court decision in force. The transfer or distribution of computer or system passwords which results in the illegitimate disclosure of personal data constitutes a crime under the Bulgarian Criminal Code (promulgated in the State Gazette No. 26 of April 2, 1968, as amended periodically) and the penalty for such a crime includes imprisonment for up to three years.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Draft Law does not introduce any rules relating specifically to e-marketing. As the Draft Law explicitly refers to the legal grounds for processing of personal data under the GDPR, thus including also the area of e-marketing, the explicit consent of the data subject is likely to be the only applicable ground for the purposes of e-marketing. The absence of a special legal framework concerning exclusively data protection in e-marketing makes the option regime the only possible legitimate method of pursuing e-marketing.

In addition, although the Draft Law repeals the provision of the current Personal Data Protection Act regulating the right of the data subject to object to any data processing for the purposes of direct marketing and does not explicitly refer to

the respective provision of the GDPR, following the direct effect of the regulation, data subjects shall still be entitled to object before the data controller or the data processor to their personal data being processed for the purposes of e-marketing.

The Bulgarian Electronic Commerce Act explicitly requires, when it comes to direct marketing to natural persons, the option mechanic to be mandatorily applied. After the natural person's consent is provided, the person shall always be given the opportunity to opt out from the direct marketing network and refuse his / her personal data to be further processed for such purposes.

ONLINE PRIVACY

Directive 2002/58 (E-Privacy Directive) is transposed into the Bulgarian Electronic Commerce Act. In 2011 the intention of the legislator was to introduce the latest amendments of Art. 5(3) under Directive 2009/136. However, the final adopted text still replicates the old wording before Directive 2009/136. The amendment itself was widely interpreted as implementing the text of Directive 2009/136 without, however, introducing the updated text.

Currently, the relevant text in the Electronic Commerce Act states that users should be provided with clear and comprehensive information about the purposes of data processing in accordance with the Personal Data Protection Act and they must be given the opportunity to refuse to the storage or access to such information. In practice the DPA interprets the law as an opt-in regime.

KEY CONTACTS

Wolf Theiss
www.wolftheiss.com/

Anna Rizova
Partner
Wolf Theiss
T +359 2 8613703
anna.rizova@wolftheiss.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BURUNDI

Last modified 28 January 2019

LAW

Burundi does not have a law that specifically regulates personal data protection. However, several laws and regulations currently in force contain data protection provisions or impose confidentiality obligations on specific types of personal information. For example, employment, banking, telecommunications and health sector laws impose some data protection requirements. Such provisions generally require covered entities to maintain the confidentiality of personal information.

- Under Law n° 1/012 of May 30, 2018 on the Code of Health Care and Health Services Provision in Burundi, healthcare institutions are required to maintain the confidentiality of patient information, unless confidentiality is waived in cases provided for by law.

- Law No. 1/17 of August 22, 2017 governing banking activities: Article 133 imposes confidentiality obligations on customer and account information. This article provides that any person who contributes to the operation, control or supervision of a banking institution is bound to professional secrecy. Violations are enforced under penal code provisions without prejudice to disciplinary proceedings.

- Several Ministerial Orders applicable to the telecommunications sector have been adopted to protect the privacy of and restrict access to and interception of the contents of communications (Legislative Decree No. 100/153 of June 17, 2013 on the Regulation of the Control and Taxation System for International Telephone Communications entering Burundi; Decree-Law No. 100/112 of April 5, 2012 on the Reorganization and Operation of the Telecommunications Regulatory and Control Agency 'ARCT'; Ministerial Ordinance No. 730/1056 of November 7, 2007 on the interconnection of telecommunications networks and services opened to the public).

DEFINITIONS

Definition of personal data

Not specifically defined.

Definition of sensitive personal data

Not specifically defined.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in Burundi.

REGISTRATION

There is no requirement to register databases.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

Most sector specific laws and regulations that impose confidentiality and data protection requirements apply to covered entities under the law or regulation, and require such entities to maintain the confidentiality of personal information during processing.

TRANSFER

No geographic transfer restrictions apply in Burundi. Certain sector specific provisions require companies to obtain consent prior to third party transfers of personal information. Notably, under Article 16 of Law n ° 1/012 of May 30, 2018 on the Code of Health Care and Health Services Provision in Burundi, "every patient has the right to decide on the use of the medical information concerning him and the conditions under which they may be transmitted to third parties."

SECURITY

There are no specific data security requirements in Burundi.

BREACH NOTIFICATION

There are no breach notification requirements in Burundi.

ENFORCEMENT

The relevant sector specific agency or regulator is generally authorized to enforce violations of confidentiality requirements.

ELECTRONIC MARKETING

There are no specific electronic marketing requirements in Burundi.

ONLINE PRIVACY

There are no specific online privacy requirements in Burundi.

KEY CONTACTS

Claver Nigarura
Managing Partner
Rubeya & Co-Advocates
T +257 22 24 89 10
claver@rubeya.bi

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CANADA

Last modified 20 May 2019

LAW

In Canada there are 28 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti-spam legislation, identity theft/ criminal code etc.) that govern the protection of personal information in the private, public and health sectors. Although each statute varies in scope, substantive requirements, remedies and enforcement provisions, they all set out a comprehensive regime for the collection, use and disclosure of personal information.

The summary below focuses on Canada's private sector privacy statutes:

- Personal Information Protection and Electronic Documents Act ('PIPEDA')
- Personal Information Protection Act ('PIPA Alberta')
- Personal Information Protection Act ('PIPA BC')
- Personal Information Protection and Identity Theft Prevention Act ('PIPITPA') (not yet in force)
- An Act Respecting the Protection of Personal Information in the Private Sector ('Quebec Privacy Act'), (collectively, 'Canadian Privacy Statutes')

PIPEDA applies to all of the following:

- Consumer and employee personal information practices of organizations that are deemed to be a 'federal work, undertaking or business' (eg banks, telecommunications companies, airlines, railways, and other interprovincial undertakings)
- Organizations who collect, use and disclose personal information in the course of a commercial activity which takes place within a province, unless the province has enacted 'substantially similar' legislation (PIPA BC, PIPA Alberta and the Quebec Privacy Act have been deemed 'substantially similar')
- Inter provincial and international collection, use and disclosure of personal information

PIPA BC, PIPA Alberta and the Quebec Privacy Act apply to both consumer and employee personal information practices of organizations within BC, Alberta and Quebec, respectively, that are not otherwise governed by PIPEDA.

DEFINITIONS

Definition of personal data

'Personal information' includes any information about an identifiable individual (business contact information is expressly "carved out" of the definition of 'personal information' in some Canadian privacy statutes.

Definition of sensitive personal data

Not specifically defined.

NATIONAL DATA PROTECTION AUTHORITY

- Office of the Privacy Commissioner of Canada ('PIPEDA')
- Office of the Information and Privacy Commissioner of Alberta ('PIPA Alberta')
- Office of the Information and Privacy Commissioner for British Columbia ('PIPA BC'), and
- *Commission d'accès à l'information du Québec* ('Quebec Privacy Act')

REGISTRATION

There is no registration requirement under Canadian Privacy Statutes.

DATA PROTECTION OFFICERS

PIPEDA, PIPA Alberta, PIPA BC and PIPITPA expressly require organizations to appoint an individual responsible for compliance with the obligations under the respective statutes.

COLLECTION & PROCESSING

Canadian Privacy Statutes set out the overriding obligation that organizations only collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Subject to certain limited exceptions prescribed in the Acts, consent is required for the collection, use and disclosure of personal information. Depending on the sensitivity of the personal information, consent may be opt in or opt out. Organizations must limit the collection of personal information to that which is necessary to fulfil the identified purposes and only retain such personal information for as long as necessary to fulfil the purposes for which it was collected.

Each of the Canadian Privacy Statutes have both notice and openness/transparency requirements. With respect to notice, organizations are generally required to identify the purposes for which personal information is collected at or before the time the information is collected. With respect to openness/transparency, generally Canadian Privacy Statutes require organizations make information about their personal information practices readily available.

All Canadian Privacy Statutes contain obligations on organizations to ensure personal information in their records is accurate and complete, particularly where the information is used to make a decision about the individual to whom the information relates or if the information is likely to be disclosed to another organization.

Each of the Canadian Privacy Statutes also provides individuals with the following:

- A right of access to personal information held by an organization, subject to limited exceptions
- A right to correct inaccuracies in/update their personal information records.

Finally, organizations must have policies and practices in place that give effect to the requirements of the legislation and organizations must ensure that their employees are made aware of and trained with respect to such policies.

TRANSFER

When an organization transfers personal information to a third party service provider (ie who acts on behalf of the transferring organization), the transferring organization remains accountable for the protection of that personal information and ensuring compliance with the applicable legislation. In particular, the transferring organization is responsible for ensuring that the third party service provider appropriately safeguards the data, and would also be required under the notice and openness/transparency provisions to reference the use of third party service providers in and outside of Canada in their privacy policies and procedures.

With respect to the use of foreign service providers, PIPA Alberta specifically requires a transferring organization to include the following information in its privacy policies and procedures:

- The countries outside Canada in which the collection, use, disclosure or storage is occurring or may occur, and

- The purposes for which the third party service provider outside Canada has been authorized to collect, use or disclose personal information for or on behalf of the organization

Under PIPA Alberta, specific notice must also be provided at the time of collection or transfer of the personal information and must specify:

- The way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada, and
- The name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization.

In addition, under the Quebec Privacy Act, an organization must take reasonable steps to ensure that personal information transferred to service providers outside Quebec will not be used for other purposes and will not be communicated to third parties without consent (except under certain exceptions prescribed in the Act). The Quebec Privacy Act also specifically provides that the organization must refuse to transfer personal information outside Quebec where it does not believe that the information will receive such protection.

SECURITY

Each of the Canadian Privacy Statutes contains safeguarding provisions designed to protect personal information. In essence, these provisions require organizations to take reasonable technical, physical and administrative measures to protect personal information against loss or theft, unauthorized access, disclosure, copying, use, modification or destruction. These laws do not generally mandate specific technical requirements for the safeguarding of personal information.

BREACH NOTIFICATION

Currently, PIPEDA, PIPA Alberta and PIPITPA are the only Canadian Privacy Statute with breach notification requirements.

In Alberta, an organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result.

Notification to the Commissioner must be in writing and include:

- A description of the circumstances of the loss or unauthorized access or disclosure
- The date or time period during which the loss or unauthorized access or disclosure occurred
- A description of the personal information involved in the loss or unauthorized access or disclosure
- An assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure
- An estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
- A description of any steps the organization has taken to reduce the risk of harm to individuals
- A description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure, and
- The name and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the loss of unauthorized access or disclosure

Where an organization suffers a loss of or unauthorized access to or disclosure of personal information as to which the organization is required to provide notice to the Commissioner, the Commissioner may require the organization to notify the individuals to whom there is a real risk of significant harm. This notification must be given directly to the individual (unless specified otherwise by the Commissioner) and include:

- A description of the circumstances of the loss or unauthorized access or disclosure
- The date on which or time period during which the loss or unauthorized access or disclosure occurred
- A description of the personal information involved in the loss or unauthorized access or disclosure

- A description of any steps the organization has taken to reduce the risk of harm, and
- Contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure

The breach notification provisions under PIPEDA are very similar to the breach notification provisions under PIPA Alberta. Under PIPEDA, organizations must also keep a record of ALL information security breaches, even those which do not meet the risk threshold of a "real risk of significant harm".

In Manitoba, PIPITPA (which is not yet in force) provides that an organization must, as soon as reasonably practicable, notify an individual if personal information about the individual that is in its custody or under its control is stolen, lost or accessed in an unauthorized manner. This requirement to notify an individual does not apply where:

- The organization is instructed to refrain from doing so by a law enforcement agency that is investigating the theft, loss or unauthorized accessing of the personal information, or
- The organization is satisfied that it is not reasonably possible for the personal information to be used unlawfully

The exact form of the notice that must be provided to individuals has not yet been prescribed.

ENFORCEMENT

Privacy regulatory authorities have an obligation to investigate complaints, as well as the authority to initiate complaints.

Under PIPEDA, a complaint must be investigated by the Commissioner and a report will be prepared that includes the Commissioner's findings and recommendations. A complainant (but not the organisation subject to the complaint) may apply to the Federal Court for a review of the findings and the court has authority to, among other things, order an organisation to correct its practices and award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Under PIPA Alberta and PIPA BC, an investigation may be elevated to a formal inquiry by the Commissioner resulting in an order. Organisations are required to comply with the order within a prescribed time period, or apply for judicial review. In both BC and Alberta, once an order is final, an affected individual has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the breach.

In Alberta and BC, a person that commits an offence may be subject to a fine of not more than CA$100,000. Offences include, among other things, collecting, using and disclosing personal information in contravention of the Act (in Alberta only), disposing of personal information to evade an access request, obstructing the commissioner, and failing to comply with an order.

Similarly, under the Quebec Privacy Act, an order must be complied with within a prescribed time period. An individual may appeal to the judge of the Court of Quebec on questions of law or jurisdiction with respect to a final decision.

A failure to comply with the Quebec Privacy Act's requirements in respect of the collection, storage, communication or use of personal information is liable to a fine of up to CA$10,000 and, for a subsequent offence, to a fine up to CA$20,000. Any one who hampers an inquiry or inspection by communicating false or inaccurate information or otherwise is liable to a fine of up to CA$10,000 and, for a subsequent offence, to a fine of up to CA$20,000.

Under the PIPITPA, it is an offence to (a) willfully collect, use, or disclose personal information in contravention of the Act, (b) wilfully attempt to gain or gain access to personal information in contravention of the Act, and (c) dispose of or alter, falsify, conceal or destroy personal information or any record relating to personal information, or direct another person to do so, with an intent to evade a request for access to information or the record. A person who commits an offence is liable on summary conviction, in the case of a person other than an individual, to a fine of not more than CA$100,000.

ELECTRONIC MARKETING

Electronic marketing is governed by both Canadian Privacy Statutes (as discussed above), as well as Canada's Anti-Spam Legislation (CASL).

Under CASL it is prohibited to send, or cause or permit to be sent, a commercial electronic message (defined broadly to include

text, sound, voice, or image messages aimed at encouraging participation in a commercial activity) unless the recipient has provided express or implied consent and the message complies with the prescribed content and unsubscribe requirements (subject to limited exceptions).

What constitutes both permissible express and implied consent is defined in the Act and regulations. For example, an organization may be able to rely on implied consent when there is an existing business relationship with the recipient of the message, based on:

- A purchase by the recipient within the past two years, or
- A contract between the organization and the recipient currently in existence or which expired within the past two years

CASL also prohibits the installation of a computer program on any other person's computer system, or having installed such a computer program to cause any electronic messages to be sent from that computer system, without express consent, if the relevant system or sender is located in Canada. In addition, the Act contains anti phishing provisions that prohibit (without express consent) the alteration of transmission data in an electronic message such that the message is delivered to a destination other than (or in addition to) that specified by the sender.

CASL also introduced amendments to PIPEDA that restrict 'address harvesting', or the unauthorized collection of email addresses through automated means (*ie*, using a computer program designed to generate or search for, and collect, email addresses) without consent. The use of an individual's email address collected through address harvesting also is restricted.

The 'Competition Act' was also amended to make it an offence to provide false or misleading representations in the sender information, subject matter information, or content of an electronic message.

CASL contains potentially stiff penalties, including administrative penalties of up to CA$1 million per violation for individuals and CA$10 million for corporations (subject to a due diligence defense). CASL also sets forth a private right of action permitting individuals to bring a civil action for alleged violations of CASL (CA$200 for each contravention up to a maximum of CA$1 million each day for a violation of the provisions addressing unsolicited electronic messages).

ONLINE PRIVACY

Online privacy is governed by Canadian Privacy Statutes (discussed above). In general, Canadian privacy regulatory authorities have been active in addressing online privacy concerns.

For example, in the context of social media, the OPC has released numerous Reports of Findings addressing issues including:

- Default privacy settings
- Social plug-ins
- Identity authentication practices
- The collection, use and disclosure of personal information on social networking sites. The OPC has also released decisions and guidance on privacy in the context of Mobile Apps

In addition, the OPC has released findings and guidelines related to the use of cookies and online behavioral advertising, including findings indicating that information stored by temporary and persistent cookies is considered to be personal information and therefore subject to PIPEDA. The OPC has adopted the same position with respect to information collected in connection with online behavioral advertising.

In 'Privacy and Online Behavioral Advertising' (the 'OBA Guidelines'), the OPC stated that it may be permissible to utilize opt-out consent in the context of online behavioral advertising if the following conditions are met:

- Individuals are made aware of the purposes for the online behavioral advertising, at or before the time of collection, in a manner that is clear and understandable
- Individuals are informed of the various parties involved in the online behavioral advertising at or before the time of collection
- Individuals are able to opt-out of the practice and the opt-out takes effect immediately and is persistent
- The information collected is non-sensitive in nature (*ie*, not health or financial information), and
- The information is destroyed or made de-identifiable as soon as possible

The OPC has indicated that online behavioral advertising must not be a condition of service and, as a best practice, should not be used on websites directed at children.

With respect to location data, such information, whether tied to a static location or a mobile device, is considered to be personal information by Canadian privacy regulatory authorities. As such, any collection, use or disclosure of location data requires, among other things, appropriate notice and consent. Most of the privacy regulatory authority decisions related to location data have arisen with respect to the use of GPS in the employment context.

The Canadian privacy regulatory authorities provide the following test that must be met for the collection of GPS data (and other types of monitoring and surveillance activities):

- Is the data demonstrably necessary to meet a specific need?
- Will the data likely be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Are there less privacy-intrusive alternatives to achieve the same objective?

KEY CONTACTS

Tamara Hunter
Associate Counsel
T +1 604.643.2952
tamara.hunter@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CAPE VERDE

Last modified 25 January 2017

LAW

Data Protection Law (Law 133/V/2001 (as amended by Law 41/VIII/2013) and Law 132/V/2001, of 22 January 2001.

DEFINITIONS

Definition of personal data

Personal data is defined as any information, regardless of its nature or the media on which it is stored, relating to an identifiable natural person (referred to as 'the data subject'). Natural persons are deemed to be identifiable whenever they can be directly or indirectly identified through such information.

Definition of sensitive personal data

Sensitive data is defined as personal data that refers to a person's:

- philosophical or political convictions
- party or union affiliation
- religious faith
- private life
- ethnic origin
- health
- sex life
- genetic information.

NATIONAL DATA PROTECTION AUTHORITY

The national data protection authority in Cape Verde is the *Comissão Nacional de Proteção de Dados Pessoais* ('data protection authority').

REGISTRATION

Pursuant to the Data Protection Law, before starting the processing of personal data (and considering the specific categories of personal data), prior authorization or registration with the data protection authority is required.

Specific prior written registration (ie authorization) granted by the data protection authority is necessary in the following cases:

- the processing of sensitive data (except in certain specific cases eg if the processing relates to data which is manifestly made public by the data subject, provided his consent for such processing can be clearly inferred from his/her statements) and only in cases where the data subject has given his/her consent to the use of such data

- the processing of data in relation to creditworthiness or solvency
- the interconnection of personal data
- the use of personal data for purposes other than those for which it was initially collected.

DATA PROTECTION OFFICERS

There is no obligation to appoint a data protection officer.

COLLECTION & PROCESSING

The collection and processing of personal data is subject to the rules laid down in the Data Protection Law. As a general note, personal data processing operations may only be undertaken once the following two requirements are met:

- the express and unambiguous consent of the data subject has been obtained
- the data protection authority has been notified.

Moreover, as previously stated, there are some cases (referred to above) in which the collection and processing of personal data is subject to prior authorization from the data protection authority.

TRANSFER

The Data Protection Law stipulates that the international transfer of personal data is only permitted if the recipient country is considered to have a sufficient level of protection in respect of personal data processing.

The sufficient level of protection for foreign countries is defined by the data protection authority.

As a general rule, the transfer of personal data to countries that do not provide for an adequate level of protection of personal data can only be permitted if the data subject has given his consent or in some specific situations, namely if the transfer:

- is necessary for the performance of an agreement between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request
- is necessary for the performance or execution of a contract entered into or to be entered into in the interest of the data subject between the controller and a third party
- is necessary in order to protect the vital interests of the data subject
- is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided the conditions laid down in law for consultation are fulfilled in the particular case.

SECURITY

The Cape Verdean Data Protection Law stipulates that data controllers must implement technical and organizational measures so as to ensure the confidentiality and security of the personal data processed. Such obligations must also be contractually enforced by the data controller against the data processor. Moreover, certain specific security measures must be adopted regarding certain types of personal data and purposes (notably, sensitive data, call recording, video surveillance etc.).

BREACH NOTIFICATION

There is no formal requirement for breach notification, nor is there formal requirement for mandatory breach notification.

ENFORCEMENT

Enforcement of the Data Protection Law is done by the data protection authority.

Moreover, the Data Protection Law sets out criminal and civil liability as well as additional sanctions for breaches of the provisions of said statute.

Civil Liability

Any person who has suffered pecuniary or non-pecuniary loss as a result of any inappropriate use of personal data has the right to bring a civil claim against the relevant party. Criminal Liability The DPL provides that all of the following constitute criminal offences:

- a failure to notify or to obtain the authorization of the DPA prior to commencing data processing operations that require such authorization
- provision of false information in requests for authorization or notification
- misuse of personal data (ie processing personal data for different purposes than those for which the notification / authorization was granted)
- the interconnection of personal data without the authorization of the DPA
- unlawful access to personal data
- a failure to comply with a request to stop processing personal data.

These offences are punishable with a term of imprisonment of up to 2 years or a fine of up to 240 days.

Additional Sanctions

The DPL also lays down sanctions that can be imposed in addition to criminal and civil liability, namely:

- a temporary or permanent prohibition on processing data
- the advertisement of a sentence applied to a specific case
- a public warning or reproach of a data controller.

ELECTRONIC MARKETING

Law 132/V/2001 provides an opt-in right for direct marketing communications. Moreover, both Law 132/V/2001 and the Data Protection Law grant data subjects the right to object to unsolicited communications, at his/her request and free of any costs, to any data processing in relation to marketing activities.

ONLINE PRIVACY

Law 132/V/2001 lays down the legal framework for data protection in the telecommunications sector. Special rules include the following:

- any personal data obtained through phone calls performed by public operators or telecommunication public service providers must be erased or made anonymous after the phone call has ended
- traffic data can only be processed for billing, customer information or support, fraud prevention and the selling of telecommunication services.

KEY CONTACTS

CV Lexis
www.mirandalawfirm.com/

Antonio Ferreira
Partner
T +238 261 13 44
praia@cvlexis.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CAYMAN ISLANDS

Last modified 28 January 2019

LAW

There is no comprehensive data protection framework currently in force in the Cayman Islands. The Legislative Assembly of the Cayman Islands passed the 2017 Data Protection Law (Law) on March 27, 2017, but this and any implementing regulations are not expected to take effect until the end of September 2019 (the date has been delayed from January 2019). The precise date the Law will come into force will be set by Cabinet Order.

Notwithstanding the lack of data protection legislation in force, the Cayman Islands recognizes a duty of confidentiality in certain circumstances, under both the common law and, implicitly, the provisions of the 2016 Confidential Information Disclosure Law (CIDL). The CIDL functions primarily to enumerate a non-exhaustive list of instances in which disclosure of confidential information may lawfully be made (see definitions below). The CIDL also repeals the previous Confidential Relationships Preservation Law (as revised) of the Cayman Islands, which regulated disclosures of confidential information by professional persons, and provided for criminal sanctions, among other penalties, for certain breaches of confidentiality on an extra-territorial basis.

DEFINITIONS

Definition of personal data

There is no definition of "personal data" contained in any legislation currently in force.

In common law, information is generally regarded as "confidential" if it has a necessary quality of confidentiality and has been either communicated or become known in such circumstances as give rise to a reasonable expectation of confidence; for example if information is obtained in connection with certain professional relationships, if it is obtained by improper means, or if it is received from another party who is subject to a duty of confidentiality.

Definition of sensitive personal data

There is no definition of "sensitive personal data" contained in any legislation currently in force.

NATIONAL DATA PROTECTION AUTHORITY

There is currently no Data Protection Authority or similar regulatory body in the Cayman Islands. However, when the Law takes effect, the Information Commissioner - who currently oversees the Freedom of Information Law - will be charged with implementing and enforcing the Law.

REGISTRATION

N/A (see National Data Protection Authority section).

DATA PROTECTION OFFICERS

There is currently no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

There are no statutory provisions currently in force that specifically address the collection and processing of personal information.

Under common law, however, it is generally a breach of confidence to misuse or threaten to misuse confidential information. The concept of misuse is a broad one, but will often include any unauthorized disclosure, examination, copying or taking of confidential information. The precise scope of the term will depend largely on the specific circumstances, including the relevant relationship and the nature of the information.

TRANSFER

Absent a breach of an obligation of confidentiality under common law, there is no statutory regulation of the transfer of information from or within the Cayman Islands. The Cayman Islands Monetary Authority (CIMA), has issued guidance in relation to the outsourcing of core functions by regulated entities to third party service providers that impacts the transfer, storage and processing of customer confidential information.

SECURITY

There are no statutory provisions in force requiring specific measures be taken to protect against or prevent disclosure, or other unlawful use of confidential information. However, a person who misuses or divulges confidential information (deliberately or otherwise) may be liable under common law.

BREACH NOTIFICATION

There are no general requirements to notify any authority or any other person of a breach of confidentiality.

ENFORCEMENT

A breach of the duty of confidentiality may give rise to a claim for, among other remedies, damages and / or an injunction. These remedies are sought through and enforced by Cayman Islands courts.

ELECTRONIC MARKETING

There are no specific restrictions addressing the use of confidential information in electronic marketing beyond those generally applicable to the use of confidential information.

ONLINE PRIVACY

There are no specific restrictions addressing online privacy beyond those generally applicable to the use of confidential information.

KEY CONTACTS

Carey Olsen
www.careyolsen.com

Nick Bullmore
Partner
T +1 345 749 2000
nick.bullmore@careyolsen.com

Graham Stoute
Counsel
Carey Olsen
T +1 345 749 2014
graham.stoute@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CHILE

Last modified 28 January 2019

LAW

Personal Data Protection is regulated in different laws.

Constitution of the Republic of Chile, Art. 19 N° 4

This law establishes individuals' constitutional right to the respect and protection of public and private life, and the honor of the person and his or her family. Also, due to a recent amendment, it includes the protection of personal data. Any person who, as a result of an arbitrary or illegal act or omission, suffers a deprivation, infringement or threat to this right may file a Constitutional Protection Action.

Law 19,628 'On the protection of private life', commonly referred as 'Personal Data Protection Law' (PDPL)

This law mainly defines and refers to the treatment of personal information in public and private databases. Last modified: Feb. 17, 2012

Law No. 20.521, about personal data protection to guarantee that information provided by credit risk entities (eg, credit agencies) is accurate, updated and true

This law forbids credit risk predictions or assessments related to late payments or contested items that are not based solely on objective data.

General Law of Banks, article 154. Banking Secrecy

This law establishes the confidentiality of transactions that individuals conduct with and through banks, applicable to the following transactions:

- Transactions covered by secrecy, which in principle implies the absolute impossibility of making them known
- Transactions covered by reserve, which implies a significant limitation on the possibility of reporting on the transaction

Law 20.575, establishes the limitations on the handling of personal data

Several principles apply to the treatment of personal financial, economic, banking or commercial data:

- Limited disclosures: This type of data shall only be communicated to established commercial entities, and only for the purpose of a credit granting process. It can also be communicated to entities that take part in this evaluation, and only for the aforementioned purpose
- Legitimacy

- Access and opposition
- Information
- Data quality
- Proportionality
- Transparency
- Nondiscrimination
- Use limitation and security in personal data treatment

Law No. 20.285, about public information access

This law prohibits including sensitive personal data in 'Active Transparency' public websites.

Decree 13-2009, from the General Secretary of Presidency

This law establishes rules under Law No. 20.285. This Decree establishes restricts disclosure of public information that contains individuals' sensitive data.

Law No. 20.169, which regulates unfair competition

This law protects competitors, consumers and, in general, any person whose legitimate interests are affected by an act of unfair competition. An act of unfair competition is any conduct contrary to good faith or good customs that, by illegitimate means, seeks to divert clientele from a market agent.

Law 19.223: Computer Crimes

This law establishes criminal sanctions for conduct related to the theft, destruction, obstruction, modification and illegal access of information contained in data processing systems.

Law No. 20.584, which regulates rights and duties related to healthcare

This law sets makes all information containing regarding healthcare procedures and treatments sensitive data.

DEFINITIONS

Definition of personal data

The only legal definition is found in the PDPL, in which **personal data** is referred to as any information concerning natural persons, identified or identifiable.

Definition of sensitive data

Under the PDPL and Decree 13-2009 from the General Secretary of Presidency, **sensitive data** means personal data relating to the physical or moral characteristics of persons or to facts or circumstances of their private or intimate life, such as:

- Personal habits
- Racial origin
- Ideologies and political opinions
- Religious beliefs or convictions
- Physical or mental health conditions, and
- Sexual life

NATIONAL DATA PROTECTION AUTHORITY

PDPL does not create a dedicated authority to supervise matters related to data protection. Issues under PDPL are resolved, generally, by Chilean courts.

Law 20.285 established the Transparency Council (*Consejo para la Transparencia*), an autonomous public body responsible for:

- Promoting transparency in public institutions
- Overseeing compliance with transparency and information disclosure standards, and
- Guaranteeing the right of access to information

REGISTRATION

Public databases must be registered in the Civil Registry and Identification Service (*Servicio de Registro Civil e Identificación*). There is no obligation to register private databases.

DATA PROTECTION OFFICERS

Under the PDPL, a Responsible Person for the registry or database should be appointed, to be responsible for decisions related to the processing of personal data. The Responsible Person is obliged to make these decisions with due diligence, taking responsibility for the damages that could occur.

COLLECTION & PROCESSING

The process of collecting and processing data is defined as any operation, complex operations or technical procedures, whether automated or not, that allows the:

- Collection
- Storage
- Recording
- Organization
- Preparation
- Selection
- Extraction
- Access
- Interconnection
- Dissociation
- Communication
- Assignation
- Transfer
- Transmission or cancellation of personal data, or
- Any other use of personal data

Personal data may be processed in the following cases:

- With written consent of data subject
- Authorized by law
- Collected from publicly accessible sources, in the the following cases:
    - It is of an economic, financial, banking or commercial nature
    - It is obtained from lists related to a specific category of people, which only disclose information such as the allegiance of such individual to such specific group, his/her profession or activity, educational degrees, address and date of birth, or
    - It is required for direct response to commercial communications or marketing, or direct sale of goods or services
    - When personal data is treated by private entities only for their exclusive internal use, or that of their associated or affiliated entities
    - In cases of processing of personal data carried out by public bodies, whenever dealing with matters within their competence, subject to the other common rules established in the PDPL

TRANSFER

Transferring is considered a form of personal data processing, so all of the aforementioned rules apply, including the consent requirements.

SECURITY

The Responsible Person is required to ensure that individuals involved in personal data processing are subject to and comply with confidentiality obligations, even after they end their contractual relationship; these individuals are liable for the security of personal data contained in databases.

For automated transmission procedures, the Responsible Person must, at all times, ensure that the rights of the data subjects are safeguarded and the transmission is related to the tasks and purposes of the participating organizations. Also, in the case of a request for personal data through an electronic network, the following information must be recorded:

- The inquirer's identity
- The motive and purpose of the request, and
- The specific data being transferred

BREACH NOTIFICATION

There is no obligation to report a data breach.

ENFORCEMENT

The data subject has the right to require that the Responsible Person provide information on:

- What data is held
- Its source and recipients
- Purpose of processing, and
- Detailed information on any person or entities to which the data is frequently sent

The data subject may also request that any incorrect or incomplete record of personal data be modified.

The data subject can request the deletion of his / her personal data, as well as revoke his / her consent to data processing. The aforementioned rights and provisions cannot be contractually waived or limited.

Requests for information, modification, etc can only be denied when the Responsible Person can show that information etc will affect:

- The duty of confidentiality
- National security, or
- Interests

In the cases mentioned above, if the Responsible Person does not reply or respond within two business days to a data subject's request, the data subject can file a complaint before local civil court. Along with specific performance, the affected individual can also claim damages.

The Responsible Person shall indemnify the data subject for the pecuniary and moral damages caused by the undue processing of the data, and must delete, modify or block the data as required by the data subject or, if applicable, ordered by the court.

The judge must reasonably determine the amount of damages, and may impose fines up to US$3,600.

In accordance with the provisions of Law 19.223 of Computer Crimes, criminal sanctions (imprisonment and fines) may be imposed for breaching information processing systems and/or revealing any information contained therein.

ELECTRONIC MARKETING

Private entities are allowed to create and maintain databases for purposes of sending marketing and promotional emails, provided that the requirements mentioned in Collection and Processing section have been fulfilled.

However, any person may require that his or her information be deleted in this case, either permanently or temporarily.

The Consumer Protection Law defines marketing and promotional communications as the communication that the provider of goods or services sends to the public by any means, in order to inform and motivate the purchase or contract for goods or services, and provides that all marketing practices must comply with the following:

- Terms and conditions and / or characteristics of the offered goods and services shall be accurate
- An 'expedited means to request' the suspension of any further communications (opt-out) shall be included in such communications
- Every marketing email must indicate that it is an advertisement, and include the identity of the sender and a valid email address to which an opt-out request may be sent

Note: Congress is currently considering Modifications of the Consumer Protection Law.

ONLINE PRIVACY

There are no laws governing online privacy or cookies. However, there is some risk that the use of cookies could implicate computer crime laws prohibiting unauthorized access to computers and information therein.

KEY CONTACTS

Albagli Zaliasnik
www.az.cl/

Felipe Bahamondez
Partner
DLA Piper BAZ | NLD Spa
T +56 2 2798 2602
fbahamondez@dlapiper.cl

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CHINA

Last modified 4 January 2019

LAW

There is not a single comprehensive data protection law in the People's Republic of China (PRC). Instead, rules relating to personal data protection and data security are part of a complex framework and are found across various laws and regulations. Provisions found in laws such as the General Principles of Civil Law and the Tort Liability Law have generally been used to interpret data protection rights as a *right of reputation* or *right of privacy*. However, such interpretation is not explicit.

On June 1, 2017, the PRC Cybersecurity Law came into effect and became the first national-level law to address cybersecurity and data privacy protection. However, there remains quite a bit of uncertainty as to how the PRC Cybersecurity Law will be applied, and what practical steps need to be taken to achieve compliance and the regulatory environment continues to evolve rapidly. Draft guidelines are currently published almost weekly, however, it is expected that some guidelines and national standards will be finalized in the coming months to further assist organizations in complying with the data protection obligations imposed under the PRC Cybersecurity Law. These include (this is not an exhaustive list):

- Draft Guidelines on Multi-Level Protection Scheme for Information Systems released on June 27, 2018;
- Draft National Standard of Information Security Technology – Guidelines for Personal Information Security Impact Assessment released on June 11, 2018;
- Draft National Standard of Information Security Technology – Guidelines on Data Security Capability Maturity Model released on September 29, 2018; and
- Draft Guideline for Internet Personal Information Security Protection released on November 30, 2018.

In addition to the PRC Cybersecurity Law, the following (together with a number of new laws and regulations released and passed to supplement the PRC Cybersecurity Law) form the backbone of general data protection rules currently in the PRC:

- The Decision on Strengthening Online Information Protection, effective from December 28, 2012 (Decision)
- National Standard of Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services, effective from February 1, 2013 (Guideline)
- National Standard of Information Security Technology – Personal Information Security Specification, effective from May 1, 2018 (PIS Specification)

The purpose of the Decision is to protect online information security, safeguard the lawful rights and interests of citizens, legal entities or other organizations, and ensure national security and public interests. The Decision has the same legal effect as a law. While the Guideline and PIS Specification are only technical guides and thus not legally binding, they are highly persuasive. Unlike the Decision (which is more of a general overview of the guiding principles relating to data protection), the Guideline and the PIS Specification cover in detail key issues such as data transfers, sensitive personal information, and data subject rights. Given the lack of binding laws and regulations which provide detailed guidance on data processing, the Guideline and PIS Specification are important references. Therefore, compliance with the Guideline and PIS Specification is recommended as best practice.

Provisions contained in other laws and regulations may also apply depending on the industry or type of information involved (for

example, personal information obtained by financial institutions, e-commerce businesses, certain healthcare providers, or telecom or Internet service/content providers is subject to special regulation). For example (this is not an exhaustive list):

- The PRC Criminal Law prohibits sale or illegal provision of, or illegal access (such as theft) to citizens' personal information;
- The Provisions on Telecommunication and Internet User Personal Information Protection (effective from September 1, 2013), which are applicable to telecom and Internet service providers;
- The Guidelines for Data Governance of Banking Financial Institutions, which are applicable to banking financial institutions established within the territory of the PRC licensed by the PRC banking regulatory authorities;
- The People's Bank of China's Circular on Further Intensifying Management of Credit Information Security (effective from May 2, 2018) setting out obligations to strengthen credit information security in relation to access to database for financial credit information;
- The PRC Consumer Rights Protection Law (effective from March 15, 2014) (Consumer Protection Law) contains data protection obligations which are applicable to most if not all types of businesses that deals with consumers. The Consumer Protection Law was supplemented by the Measures on Penalties for Infringing Upon the Rights and Interests of Consumers (effective from March 15, 2015).
- Further, the draft Implementation Regulations for the PRC Consumer Protection Law released on 5 August 2016 will, if implemented, reiterate and clarify some of the data protection obligations as regards consumers' personal information; and
- The PRC E-Commerce Law (effective from January 1, 2019), reiterating requirements to protect personal information in an e-commerce context (E-commerce Law).

Applicability of other laws or regulations will invariably depend on the factual context of each case and further independent analysis is recommended, (for example, businesses in the banking, healthcare or securities sectors may be subject to industry-specific data protection regulations; and employee personal data attracts some protections under employment laws).

Finally, the above only refers to national level laws. Provincial level laws may also need to be considered.

DEFINITIONS

Definition of personal data

There is no single, pervasive definition of personal data in the PRC, but the concept of personal data in the various laws, regulations and guidance that comprise the data protection framework in the PRC are starting to become more aligned.

In summary, personal data (which is generally referred to as ‘personal information’ in the PRC) means all kinds of information (including sensitive personal information) recorded by electronic means or otherwise that can be used to independently identify or be combined with other information to identify a natural person's information.

Definition of sensitive personal data

Similar to personal information, there is no single, pervasive definition under binding laws in the PRC for sensitive personal data (which is generally referred to as 'sensitive personal information' in the PRC).

However, the PIS Specification – which as noted above is a non-binding, highly persuasive standard – provides some distinction between sensitive personal information and general personal information. Sensitive personal information is defined in the PIS Specification as personal information which, if disclosed or abused, will lead to adverse impact to the data subject. Examples of sensitive personal information as set out in the PIS Specification include personal identification number, mobile phone number, individual biometric information, bank account number, correspondence records and contents, property information, credit information, location tracking, lodging information, health and physiological information and transaction information etc.

NATIONAL DATA PROTECTION AUTHORITY

The Cyberspace Administration of China (CAC) is currently considered the primary data protection authority in the PRC, although there are also enforcement regulators such as the Ministry of Public Security, and sector-specific regulators that may

monitor and enforce data protection issues, such as the People's Bank of China or China Banking Regulatory Commission which regulate banks and financial institutions.

REGISTRATION

There is no legal requirement in the PRC for data users to register with the data protection authority.

DATA PROTECTION OFFICERS

There is no general requirement under binding PRC laws for organizations to appoint a data protection officer.

However, the PIS Specification requires that an organization to appoint a data protection officer and a data protection department if the organization's main business line involves data processing and the organization has either:

- more than 200 employees
- personal information of more than 500,000 individuals are processed, or personal information of more than 500,000 individuals is expected to be processed within 12 months

COLLECTION & PROCESSING

In general, express consent is required from the data subject before personal information can be collected, used, transferred or otherwise processed. In certain circumstances, such as collecting or processing sensitive personal information, overseas data transfers and direct marketing, specific consent (i.e., consent specific to the processing activity/transfer (rather than just general consent to the privacy notice, expressed through an affirmative action) is required from the data subject. As a matter of best practice, and given the wide definition of sensitive personal information, explicit consent is recommended.

In addition, a data controller (i.e. the organization who has the authority to determine the purposes, means or method of processing) should provide data subjects with a privacy policy or other form of notice, informing them of the scope and ways in which their personal data is collected, processed and disclosed, including the following information:

- the identity of the data controller, including its registered name, registered address, principal office, a telephone number and/or an e-mail address
- a list of personal information collected for each business purpose, location of storage, retention period, means and scope of the personal information collected
- the purposes sought by the data controller, i.e., what the data controller uses the data for (for instance, supplying goods and services, creating a user account, processing payments, managing subscriptions to the newsletters, etc.). These should be comprehensive, as additional purposes will require new consent
- circumstances under which the data controller will transfer, share, assign personal data to third parties or publicly disclose personal data, the types of personal data involved in the sharing, assignment or disclosure, and the types of third party data recipients
- data security capabilities of the data controller, as well as the data protection measures to be adopted by the data controller
- the rights of data subjects and mechanisms for them to exercise these rights, e.g. methods to access, rectify, delete their personal information, methods to de-register their accounts, withdraw their consent, and to obtain copies of their personal information, methods to restrict automated decision by the data system etc., and
- potential risks for providing personal data, as well as possible impacts for not providing the data; and channels and mechanism for making inquiries and lodging complaints by data subjects, as well as external dispute settlement body and contact information.

The information in the privacy policy must be true, accurate and complete. The contents of the privacy policy must be clear and easy to understand, and ambiguous language should be avoided. The privacy policy should be made available to the data subject when collecting consent, and published publicly and easily accessible. When changes occur to the information provided in the privacy policy, the data subject should be notified of such changes and further consent may need to be obtained.

Collection from individuals under 14 years old is prohibited unless explicit consent is obtained from their legal guardians.

TRANSFER

If a data controller wishes to share, disclose or otherwise transfer an individual's personal information to a third party (including group companies), the data controller must:

- not share or transfer any personal biometric information or other types of particularly sensitive personal information where prohibited under relevant laws or regulations
- perform a personal information impact assessment, and take effective measures to protect the data subjects according to the assessment results (for example putting in place a data transfer agreement or similar contractual protections)
- inform the data subject of the purposes of the sharing, disclosure or transfer of the personal information and the types of data recipient, and obtain prior express consent from the data subject
- record accurately and keep the information in relation to the sharing, disclosure or transfer of the personal information, including the date, scale, purpose and basic information of the data recipient of the sharing or assigning

Cross-border transfers

Where the sharing, disclosure or transfer of the personal information is to a third party outside of the PRC additional rules will apply. Data localization is an increasing trend in the PRC, with various draft measures as well as sector specific regulations prohibiting the transfer of certain personal information outside the borders of the PRC – although to what extent these rules apply remains unclear and further clarification from the regulators is expected.

Under the current prevailing understanding, in order to transfer or access personal information outside of the PRC, the data controller must:

- inform the data subject of the transfer outside of the PRC, and obtain explicit consent of the data subject before the personal information is shared, disclosed or transferred
- store a copy of the data within the PRC
- conduct a security assessment (in addition to the personal information impact assessment described above), which is likely to be a self-assessment but for those organizations deemed critical information infrastructure operators (CIIO) regulatory input may be required,

In addition to the above requirements, additional restrictions apply to transfers of certain information outside of the PRC:

- certain personal information within prescribed thresholds (yet to be finalized) may still not be able to leave the PRC
- certain personal information governed by sector specific regulations, such as banking and online mapping, may also not leave the PRC
- certain categories of regulated (personal and non-personal) data are not permitted to leave the PRC at all, such as 'important data' and state secrets.

SECURITY

Organizations must take appropriate technical and organizational measures against unauthorized or unlawful processing and against accidental loss, destruction of, or damage to, personal information. The measures taken must ensure a level of security appropriate to the harm that may result from such unauthorized or unlawful processing, accidental loss, destruction or damage, and appropriate to the nature of the data.

Under the PRC Cybersecurity Law, network operators (i.e. organizations that own or operate IT networks/infrastructure and, it is thought, even just websites in China) must implement technical and other necessary measures to ensure the security of personal information and to prevent the data from being accidentally disclosed, tampered with or destroyed. Remedial measures must be taken immediately if personal information is being or is likely to be disclosed, tampered with or destroyed. Network operators should also establish systems to handle complaints or reports about personal information security, publish the means for individuals to make such complaints or reports, and promptly handle any such complaints or reports received. Organizations deemed CIIOs (see above) must apply additional security safeguards.

The PRC Cybersecurity Law implemented a multi-level protection scheme for cybersecurity protection of information systems by

network operators. Information systems are classified into 5 tiers and the security standard goes higher from tier 1 to tier 5. Organizations should conduct a self-evaluation and determine the tier(s) to which its information systems belong, based on relevant laws, regulations and guidelines, including the Classification Guide for Classified Protection of Information System. Filing to the Public Security Bureau is required and, in certain circumstances, assessment by accredited third party may also be required, depending on the determined tier level of a respective information system. Further guidelines and draft measures have been published recently to provide further details and requirements on the process and technical aspect of the tiered system.

If a data controller appoints a data processor to process personal information on its behalf, the data controller should ensure sufficient measures are adopted by the data processor to protect the personal information: for example, to conduct due diligence and regular audits on data processor to ensure the data processor adopts sufficient and adequate security measures; and put in place an appropriate data processing agreement with the data processor.

BREACH NOTIFICATION

The PRC Cybersecurity Law introduced a general requirement for the reporting and notification of actual or suspected personal information breaches. Where personal information is leaked, lost or distorted (or if there is a potential for such incidents), organizations must promptly take relevant measures to mitigate any damage and notify relevant data subjects and report to relevant government agencies in a timely manner in accordance with relevant provisions.

The PRC Cybersecurity Law does not prescribe a timeline for reporting personal information breaches or security incidents. However, the PIS Specification and other guiding circulars (such as the National Network Security Incident Contingency Response Plan) provide some guidelines on the reporting and notification of personal information breaches or security incidents.

Organizations should also adopt proactive measures to minimize the risk of personal information breaches or security incidents, including but not limited to, formulating a contingency plan, organizing trainings and conducting regular contingency drills.

ENFORCEMENT

Possible enforcement of, and sanctions for, a data protection breach in the PRC will depend on the specific data protection laws and regulations breached. Sanctions in relation to data protection breaches are scattered across various different laws and regulations, and the measures described below may not be comprehensive in all situations, as additional laws or regulations may be applicable depending on the industry or type of information at hand.

Typically, it would be a graded approach - warning and requirement to comply, then possibly fines up to approximately RMB 500,000. Affected individuals may also potentially claim for indemnification under the Tort Liability Law. In severe cases, breaches may lead to higher fines being imposed or the revocation of license. Responsible personnel could be prohibited from engaging in relevant business and their conduct could be recorded in their social credit files. Depending on the severity of the illegal conduct, the responsible person could also be subject to detention or up to seven years of imprisonment, plus a concurrent fine to the organization if applicable.

The enforcement environment is evolving rapidly as individuals are increasingly aware of their data protection rights and as data protection obligations expand as laws develop and are added in China. For example, the PRC Cybersecurity Law suggests the possibility of ordering corrections, issuing warnings, confiscation of illegal gains and fines of up to 10 times of illegal gains (or fines of up to RMB 1,000,000 where there is no illegal gain) upon discovery of violation in handling personal information. The responsible persons may also be fined between RMB 10,000 to 100,000.

ELECTRONIC MARKETING

Direct marketing by electronic means is only possible if the targeted consumers have explicitly consented to receiving such messages either at the time their electronic address/mobile phone number was collected or at a later time.

Specific information must be stated in each electronic message: for example, the identity of the entity sending the message, and a mark identifying "(advertisement in Chinese)" or "AD" on a direct marketing message.

There are also specific rules applicable to direct marketing by text messages (SMS), and certain specific prescribed information

must be provided to data subjects at the time their mobile phone number was collected or prior to sending direct marketing text messages.

ONLINE PRIVACY

The PRC Cybersecurity Law, Consumer Protection Law and E-Commerce Law offer similar protection to consumer/user personal information. Data controllers should strengthen management of information provided by users, prohibit the transmission of unlawful information and take necessary measures to remove any infringing content, then report to supervisory authorities. Sufficient notice and adequate consent should be obtained from data subjects prior to the collection and use of personal information. Further obligations are imposed on mobile apps providers including but not limited to conducting real-name identification, undertaking information content review.

Under the PRC Cybersecurity Law, Consumer Protection Law, E-Commerce Law and the PIS Specification, data subject have specific rights, such as, to access their data, to correction of their data, to request deletion of data in the event of a data breach, to de-register their account etc.

There are currently no specific requirements regarding cookies within existing laws or regulations in the PRC. However, the use of cookies and/or similar tracking technologies, to the extent they constitute processing of personal information, should be notified to data subjects as part of a privacy policy and adequate consent should be obtained from data subjects for such use.

KEY CONTACTS

Scott Thiel
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +852 2103 0519
scott.thiel@dlapiper.com

Carolyn Bigg
Of Counsel
T +852 2103 0576
carolyn.bigg@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

COLOMBIA

Last modified 28 January 2019

LAW

Colombia recognizes two fundamental personal data rights under Articles 15 and 20 of its Constitution: the right to privacy and the right to data rectification. Personal data processing is further regulated by two statutory laws and several decrees that set out data protection obligations.

Statutory Law 1266 of 2008 (Law 1266) regulates the processing of financial data, credit records and commercial information collected in Colombia or abroad. Law 1266 defines general terms on habeas data and establishes basic data processing principles, data subject rights, data controller obligations and specific rules for financial data.

Law 1266 regulates the terms User of Data and Data Operator. 'User of Data' is a person or entity who accesses databases and uses the information it has gathered. 'Data Operator' is a person who manages a database. Under the law a 'Data Controller' is a legal or natural person responsible for data treatment, or processing, and a 'Data Processor' is a legal or natural person in charge of personal data processing. The Data Controller creates databases on its own or in association with others, while the Data Processor processes personal data on behalf of the Data Controller. Nevertheless, an entity may be regarded as both Controller and Processor of personal data.

Law 1266 further requires Data Controllers and Data Processors to guarantee that personal data: is maintained pursuant to strict security measures and confidentiality standards, will not be modified or disclosed absent prior data subject consent, and will only be used for purposes identified in a privacy policy or notice.

Statutory Law 1581 of 2012 (Law 1581) regulates personal data processing, as well as databases. Law 1581 defines special categories of personal data, including sensitive data and data collected from minors. The law further regulates data processing authorization and procedures, and creates the National Register of Data Bases (NRDB). Law 1581 is applicable to all data collection and processing in Colombia, except data regulated under Law 1266 and certain other types of data or regulated industries. The law is further applicable in any case where a data processor or controller is required to apply Colombian law under an international treatise.

Law 1581 does not regulate:

- Databases regulated under Law 1266
- Personal or domestic databases
- Databases aimed to protect and guarantee national security, prevent money laundering and terrorism financing
- Intelligence and counter-intelligence agency databases, and
- Databases regulated under Law 79 of 1993 (on population census)

Decree 1377 of 2013 (Decree 1377), is a piece of secondary regulation related to Law 1581 which outlines requirements for personal and domestic databases regarding authorization of personal data usage and recollection, limitations to data processing, cross-border transfer of data bases and privacy warnings, among others. This Decree also requires that controllers and processors

to adopt a privacy policy and privacy notice.

Decree 886 of 2014 (Decree 886) and Decree 090 of 2018 (Decree 090) issued by the Ministry of Commerce, Industry and Tourism as well as the Resolution 090 of 2018 issued by the Superintendence of Industry and Commerce, regulate the National Register of Data Bases and sets deadlines for registration of existing data bases in Colombia.

DEFINITIONS

The Colombian data protection regime distinguishes between personal data and a sub-category of sensitive personal data, depending on the information and the harmful effects caused by its unlawful use. Law 1266 and Law 1581 contain particular rules related to sensitive personal data.

Definition of personal data

Under Law 1266, personal data is defined as any information related to or that may be associated with one or several determined or determinable natural or legal persons. Personal data may also be regarded as public, private or semi-private data. Public data is available to the public based on a legal or constitutional mandate. Private or semi-private data is data that does not have a public purpose, is intimate in nature and the disclosure of which concerns only the data subject.

Under Law 1581, personal data is defined as any information related to, or that may be related to, one or several determined or determinable individuals, meaning natural persons only.

Definition of sensitive personal data

Under Law 1266, sensitive personal data is defined as data that due to its sensitivity is only relevant to its owner.

Under Law 1581, sensitive personal data is any data that affects its owner's intimacy or whose improper use might cause discrimination. Data that reveals any of the below information is considered sensitive data and its processing is forbidden by law:

- Ethnic or racial origin
- Political orientation
- Religious or philosophic convictions
- Membership in labor unions, human right groups or social organizations
- Membership in any group that promotes any political interest or that promotes the rights of opposition parties
- Information regarding health and sexual life, and
- Biometrics

Sensitive data shall only be processed:

- With a special and specific authorization given by the data subject
- When it is necessary to preserve the data subject's life, or a vital interest and such data subject is physically or legally unable to provide authorization
- When it is data used for a legitimate activity and with all necessary security measures, by an NGO, an association or any kind of nonprofit entity, in which case, the entity will need an authorization granted by the data subject to provide the data to third parties
- When the data is related to or fundamental to the exercise of a right in the context of a trial or any judicial procedure, or
- When the data has a historic, statistical or scientific purpose, in which case the identity of the data subject must not be disclosed

NATIONAL DATA PROTECTION AUTHORITY

According to Law 1266, there are two different authorities on data protection and data privacy matters. The first of them, which acts as a general authority, is the Superintendent of Industry and Commerce (SIC). The second authority is the Superintendence of Finance (SOF), which acts as a supervisor of financial institutions, credit bureaus and other entities that manage financial data or credit records and verifies the enforcement of Law 1266.

Nevertheless, under Law 1581, the SIC is the highest authority in personal data protection and data privacy. It is empowered to investigate and impose penalties on companies for the inappropriate collection, storage, usage, transfer and elimination of personal data.

REGISTRATION

Law 1581 created the National Register of Data Bases (NRDB). Databases that store personal data and whose automated or manual processing is carried out by a natural or legal person, whether public or private in nature, in the Colombian territory or abroad, shall be registered in the NRDB. Database registration is also required if Colombian law is applicable to the data controller or data processor in accordance with an International Law or Treaty. Registration is mandatory for data controllers that are either of the following:

- Companies or nonprofit entities that have total assets valued above 100,000 Tax Value Units (TVU), meaning COP$3.32 billion (USD$1.1 million)[1]
- Legal persons of public nature

Decree 866 states that each data controller shall register each one of its databases, independently and must distinguish between manual and automatized databases. In addition, in order to register each database, the data controller or data processor shall provide the following information:

- Identification information of the data controller, such as: business name, tax identification number, location and contact information
- Identification details of the data processor, such as: business name, tax identification number, location and contact information
- Contact channels to grant data subjects rights
- Name and purpose of the database
- Form of processing (manual / automatized)
- Security standards
- Privacy policy

According to Decree 090, the following data controllers had to register their databases between September 2018 and January 2019:

- Companies or nonprofit entities with total assets of a value greater than 610,000 TVU shall have been registered by September 30, 2018.
- Companies or nonprofit entities with total assets of a value greater than 100,000 and up to 610,000 TVU shall have been registered by November 30, 2018.
- Legal persons of public nature shall be registered by January 31, 2019.

Any new database must be registered within two months following its creation. Finally, the data controller has the obligation to update the information contained in each database's registry.

---

[1] Based on the Tax Value Unit for 2018 (COP$33,156 (USD $11)). The Tax Value Unit is updated yearly by the Colombian tax authority.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer in Colombia.

COLLECTION & PROCESSING

The processing of financial data, credit records and commercial information, collected in Colombia or abroad, does not require authorization from the data subject. This information may only be disclosed to:

- The data subject or authorized third parties, pursuant to the procedure established by law
- The Users of the Data
- Any judicial or jurisdictional authority upon request
- Any control or administrative authority, when an investigation is ongoing
- Data processors, whether with the data subject's authorization, or when no authorization is needed if, and the database aims for the same objective or involves an activity that may cover the purpose of the disclosing data processor

On the contrary, Law 1581, requires the authorization of the data subject in order for the data controller to process private and semi-private personal data. For the authorization to be valid it shall be prior to the data processing and shall be informed, meaning that the data subject shall be aware of the exact purposes for which the data is being processed. Decree 1377 requires the following:

- Personal data shall only be collected and processed in accordance with the purposes authorized by the data subject.
- Such authorization shall be obtained by any means, provided that it allows subsequent consultation.

Authorization is not required when:

- The information is demanded by a public or administrative entity by means of a judicial order or exercising its legal duties.
- It is public data.
- A medical or sanitary urgency demands the personal data processing.
- The data processing is authorized by law for historical, statistic or scientific purposes.
- The data is related to people's birth certificates.

Regarding sensitive data, Section 6 of Decree 1377 states that the data controller shall do the following:

- Expressly inform to the data subject that he or she is not compelled to provide sensitive data, and
- Obtain his / her prior and express consent prior to the sensitive data processing

In any case, silence will be deemed as a reasonable means of obtaining authorization for personal or sensitive data processing.

Furthermore, when collecting personal data of children the data controller and the data processor shall ensure that personal data processed serves and respects the children's superior interests and guarantees their fundamental rights. For these purposes, the authorization for processing a child's data shall be provided by his or her legal representative.

Privacy policy and privacy notice

Decree 1377 establishes the obligation for data controllers to develop a privacy policy that governs personal data processing and ensures regulatory compliance. For this reason, privacy policies are mandatory for all data controllers and shall be clearly written; Spanish is recommended. Finally, according to the Decree 1377, the minimum requirements for the privacy policy are:

- Name, address, email and phone number of the data controller
- Processes and handling of data and the purpose of such processing
- Rights of the data subject
- Individual or department within the data controller that is responsible for the attention to requests, consultations and claims to update, rectify or suppress data and to revoke authorization
- Procedure to exercise the abovementioned rights, and
- Date of creation and effective date

The privacy notice is a verbal or written communication by the data controller, addressed to the data subject, for processing her/his personal data. In this communication, the data subject is informed about the privacy policies of the data controller, the manner to access them and the purposes of the treatment.

TRANSFER

Per Law 1581, the transfer of personal data occurs when the data controller or the data processor located in Colombia sends the

personal data to a recipient, in Colombia or abroad, who is responsible for the personal data, *ie*, a data controller.

Cross-border data transfer is prohibited unless the country where the data will be transferred meets at least the same data privacy and protection standards as those in Colombian regulation. In this regard, adequate levels of data protection will be determined in accordance with the standards set by the SIC.

This prohibition does not apply in the following cases:

- When the data subject has expressly consented to the cross-border transfer of data
- Exchange of medical data
- Bank or stock transfers
- Transfers agreed under international treaties to which the Colombia is a party
- Transfers necessary for the performance of a contract between the data subject and the controller, or for the implementation of pre-contractual measures, provided the data owner consented, and
- Transfers legally required in order to safeguard the public interest

Therefore, the data controller requires the authorization of the data subject for transferring the personal data abroad, unless such transfer is to one of the following countries which, according to the SIC, meet the standard of data protection and security levels.

Authorized countries for international transfer of personal data

- Austria
- Belgium
- Bulgaria
- Costa Rica
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungry
- Iceland
- Ireland
- Italy
- Japan
- Latvia
- Lithuania
- Luxembourg
- Malta
- Mexico
- Netherlands
- Norway
- Perú
- Poland
- Portugal
- Republic of Korea
- Romania
- Serbia
- Slovakia
- Slovenia

- Spain
- Sweden
- United States
- United Kingdom

The SIC also considers that personal data can be transferred to any country regarding which the European Commission considers to meets its standard for levels of protection.

Transmission of personal data

The transmission of personal data takes place when the data controller provides personal data to a data processor, in Colombia or abroad, in order to allow the data processor to process the personal data on behalf of the data controller. The data subject's consent is required for the transmission of data, unless there is an adequate data transfer agreement in place between the data processor and the data controller.

In this regard, Decree 1377 requires that the aforementioned agreement include the following clauses:

1. The extent and limitations of the data treatment
2. The activities that the data processor will perform on behalf of the data controller, and
3. The obligations the data processor has to data subjects and the data controller

The data processor has three additional obligations when processing personal data:

- Process data according to the legal principles established in Colombian law
- Guarantee the safety and security of the databases
- Maintain strict confidentiality of the personal data

The data controller that transmits data to a data processor must identify the data processor in the National Database Register for each database transmitted. Finally, the data processor must process the personal data in accordance with the data controller's privacy policy and the authorization given by the data subject.

SECURITY

Data controllers have the legal duty of guaranteeing that the information under their control is kept under strict security measures. For this reason, they shall ensure that such information will not be manipulated or modified without the authorization of the data subject. Indeed, the data controller shall develop an information security policy that prevents the unauthorized access, the damage or loss of information, including personal data.

BREACH NOTIFICATION

Under section 17. and section 18. of Law 1581, both the data controller and the data processor shall notify the authority (SIC) if there is a breach of security, a security risk, or a risk for data administration.

ENFORCEMENT

Since privacy and proper maintenance of personal data are fundamental constitutional rights in Colombia, every citizen is entitled to pursue protection before any Colombian judge, via constitutional action. Any judge may order a private or public entity to modify, rectify, secure or delete personal data if it is kept under conditions that violate constitutional rights. Constitutional actions can take up to ten days to be resolved and an order issued and failure to comply may result in imprisonment of the legal representative of the violating entity.

The Criminal Code of Colombia sets out in section 269F that anyone who, without authorization, seeking personal or third party gain, obtains, compiles, subtracts, offers, sells, interchanges, sends, purchases, intercepts, divulges, modifies or employs personal codes or data contained in databases or similar platforms, will be punishable by 48 to 96 months of prison, and a fine of (approximately US$20,000 to US$200,000).

Finally, since SIC is an administrative and jurisdictional authority, it is allowed to investigate (as mentioned above), request information, initiate actions against private entities, and impose fines up to approximately US$400,000, and order or obtain temporary or permanent foreclosure of the company, entity or business.

ELECTRONIC MARKETING

Law 527 of 1999 (Law 527) regulates e-commerce and electronic marketing. Authorization of the data subject is required for types of marketing, whether electronic or other.

ONLINE PRIVACY

Personal data must not be available online unless there are adequate security measures to ensure that access by any unauthorized user is restricted.

The use of cookies in web pages is forbidden unless the data subject has given an authorization for usage which may be obtained by a pop-up informing the user about the privacy policy and the way to disable cookies. All the other tracking systems need proper authorization from the data subject.

KEY CONTACTS

Maria Claudia Martinez Beltrán
Associate Director
DLA Piper Martinez Beltrán
T +57 3174720
mcmartinez@dlapipermb.com

Daniela Huertas
Junior Associate
DLA Piper Martinez Beltrán
T +57 3174720
dhuertas@dlapipermb.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

COSTA RICA

Last modified 28 January 2019

LAW

Data privacy regulation in Costa Rica is contained in two laws, the "Laws": Law No. 7975, the Undisclosed Information Law, which makes it a crime to disclose confidential and/or personal information without authorization; and Law No. 8968, Protection in the Handling of the Personal Data of Individuals together with its by-laws, which were enacted to regulate the activities of companies that administer databases containing personal information. Therefore, the scope of the second law is limited.

DEFINITIONS

Definition of personal data

Personal information contained in public or private registries (*eg*, medical records) that identifies or could be used to identify a natural person. Personal information can only be disclosed to persons or entities with a need to know such information.

Definition of sensitive personal data

Personal information related to the personal sphere of an individual, including racial origin, political opinion, religious or spiritual convictions, socioeconomic condition, biomedical or genetic information, sex life and sexual orientation, among others. Sensitive personal data cannot be disclosed without express prior authorization from the data subject.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to Law No. 8968, the Agency for the Protection of Individual's Data (PRODHAB) is the entity charged with enforcing compliance with the Laws.

The Constitutional Court also has jurisdiction to hear claims alleging violations of the Laws.

REGISTRATION

Under Law 8968, companies that manage databases containing personal information and that distribute, disclose or commercialize such personal information in any manner must register with the Agency.

Entities that manage databases containing personal information for internal purposes do not need to be registered with PRODHAB.

Databases managed by financial institutions subject to control and regulation from the Superintendent of Financial Entities of Costa Rica do not need to be registered with the Agency.

In-house databases are outside the scope of enforcement of the Laws.

DATA PROTECTION OFFICERS

There is no requirement for a data protection officer.

COLLECTION & PROCESSING

Any company may store personal information and manage a database containing it if the following rules are respected:

- When collecting personal information, private companies and/or the government must respect the "sphere of privacy" to which all individuals are entitled
- Such companies must obtain prior, unequivocal, express and valid consent from the owner of the personal information or his or her representative. Such consent must be written (either handwritten or electronic)
- Companies that maintain personal information about others in their databases must ensure that such information is:
    - Materially truthful
    - Complete and
    - Accurate
- Data subjects must be given access to their personal information and are entitled to dispute any erroneous or misleading information about them at any time
- Companies that manage databases containing personal information and that distribute, commercialize or widespread such personal information in any manner, must comply with Law 8968. Particularly, they must comply with the following:
    - Report and register the company and the database with PRODHAB
    - Report the technical measures to secure the database
    - Protect and respect confidentiality of personal information
    - Secure the information contained in the databases
    - Establish a proceeding to review requests filed by data subjects for the amendment of any error or mistakes in the database

TRANSFER

The transfer of personal information is authorized by the Laws if the data subject provides prior, unequivocal, express and valid written consent to the company that manages the database. Such transfers cannot violate the principles and rights granted in the Laws. Also, there are specific limitations regarding cross-border transfers of personal information.

The transfer of personal information from the person responsible for a database to a service supplier, technological intermediary, or entities in the same economic interest group is not considered a transfer of personal information and thus does not need authorization from the data subject. Also, the transfer of public information (which can be generally accessed) does not need authorization from the data subject.

SECURITY

Any company or individual using and / or managing personal information must take all necessary steps (technical and organizational) to guarantee that the information is kept in a secure environment, and must issue an internal protocol indicating all the procedures that shall be followed during the recollection, storage and use of such information.

If security is breached because of improper management or protection, then the responsible company may be held liable, and may

be subject to penalties and civil liability for any harm.

BREACH NOTIFICATION

Any entity managing personal data must inform PRODHAB and the data subject about any breach of personal information within five business days after the time of the breach.

In the notification, the entity must provide to PRODHAB and the data subject the following information:

- Nature of the breach
- Personal data compromised by the breach
- Immediate corrective actions taken by the see above
- Other preventive and corrective actions that will be taken
- Contact information to obtain further information

ENFORCEMENT

PRODHAB has begun to enforce the obligations established under the Laws. Individuals may file their claims directly with PRODHAB, which may initiate an administrative procedure against the database manager.

ELECTRONIC MARKETING

General rules of data protection will apply. There is little to no regulation of electronic marketing.

Notwithstanding the above, the Telecommunications Act set the scope and the mechanisms of regulation for telecommunications (including e-marketing), by describing the data subject's rights, interests and privacy protection policy. Therefore, pursuant to such Act, marketing companies may not advertise via phone nor email unless they obtain prior and express written consent from the data subject. If such companies do not comply with such condition, they might be sanctioned with a fine that can be between 0,025% and 0,5% of the income of the company of the last fiscal year.

ONLINE PRIVACY

There has been little to no regulation in this area. However, the general rules of data protection issued by the Constitutional Court, with respect to the collection and processing of personal information, apply.

KEY CONTACTS

FACIO & CAÑAS
www.fayca.com/

Carlos J. Oreamuno
Partner
T +(506) 2233 9202
coreamuno@fayca.com

Sergio A. Solera
Partner
ssolera@fayca.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CROATIA

Last modified 16 October 2018

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Act on the Implementation of the General Data Protection Regulation (in Croatian as *Zakon o provedbi Ope uredbe o zaštiti podataka*) was enacted in the Croatian Parliament on April 27, 2018 and came into force on May 25, 2018 (the '**Act** ').

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal**

convictions and offences (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Act refers to all definitions as stated in the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Croatian Personal Data Protection Agency (in Croatian as *Agencija za zaštitu osobnih podataka*).

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

The Act does not impose any special registration requirements, save for those imposed by the GDPR.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Act does not contain any special requirements related to data protection officers, other than those imposed by the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which

the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

In application of the possibility left to Member States to deviate from the provisions of the GDPR, the Act provides the following obligations with regards to the collection and processing of personal data:

Processing of Genetic Data

The Act forbids any processing of genetic data for the purposes of life insurance calculations and entering into life insurance agreements. Consent given by data subjects does not validate this restriction.

Processing of Biometric Data

Public authorities and private entities may process biometric data only if such processing is defined by law and is necessary for the protection of persons, assets, classified information or professional secrets, provided that the interests of data subjects that contravene such processing do not prevail. Processing of biometric data necessary for fulfilment of international treaties related to identification of data subjects during crossing of state borders is considered as lawful.

Private entities may process biometric data for the purposes of safe identification of users of services, only based on explicit consent given by the users in accordance with the provisions of the GDPR.

Processing of biometric data (eg fingerprints, eye-scans) for the purposes of working time recording or entry/exit of working premises is allowed only on the basis of a legal obligation or if the employer has provided an alternative mechanism for such purposes (e.g. signature list) and the data subjects provided an explicit consent in accordance with the provisions of the GDPR.

Processing of Personal Data through Video Surveillance

Data controllers (or processors) must provide a clear notification to data subjects that premises (or part of it) is under video surveillance. Such notification must be visible while entering the perimeter of surveillance at the latest, and contain the information provided in Article 13 of the GDPR. Also, a clear and understandable photograph (sticker) must be attached to the notification containing:

- a notice that the object is under video surveillance
- information on the data controller, and
- contact details of the data controller for possible complaints

Records of video surveillance may be kept for 6 months, unless a special law or regulation provides a longer period.

In relation to work premises, such premises may be put under video surveillance by the employer only if the conditions under the work safety regulations have been met, and all employees have been notified in advance on the existence of video surveillance. Premises intended for rest, hygiene and changing room may not be put under video surveillance.

In relation to residential buildings, video surveillance may be installed in such buildings under the condition that 2/3 of all owners agree. However, only access to the building's entrance and exit and common premises (eg stairways) may be put under video surveillance. Video surveillance used for the purposes to control the effectiveness of cleaners and other staff working in residential building is forbidden.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Act does not contain any special transfer requirements other than those prescribed by the GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for

ensuring the security of the processing.

The Act does not contain any special security requirements other than those prescribed by the GDPR.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Act does not contain any special breach notification requirements other than those prescribed by the GDPR.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The Croatian Personal Data Protection Agency is the enforcement body in Croatia competent for matters related to privacy and personal data. Its decisions may be challenged by initiating administrative litigation at the competent administrative court.

Administrative fines may not be imposed to public authorities and bodies.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate

clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Electronic marketing is regulated by the DP Law. A data controller has to inform a data subject in advance on intention to collect and process his/her data for marketing purposes. A data subject can decline to give his / her consent for the respective processing. However, even if a data subject consents to the particular processing for the respective purposes, the processing is allowed only for as long as the data subject does not oppose the same (opt-out provisions are commonly used in consent forms).

The Act does not contain any special electronic marketing requirements other than those prescribed by the GDPR. It sets the consent age limit for offering of information society services to children to 16.

ONLINE PRIVACY

All rules on data protection are applicable to the electronic communication and online privacy as well. AZOP is in charge of control of all online data processing.

Online privacy and cookies are regulated by the Electronic Communications Act ('Official Gazette of the Republic of Croatia', nos. 73/2008, 90/2011, 133/2012, 80/2013 and 71/2014) which has implemented Directive 2002/58/EZ on personal data processing and privacy protection in electronic communications sector.

Usage of electronic communication network for data storage or access to already stored data in terminal data subject equipment is allowed only with a data subject's consent after he / she was clearly and completely informed on the purpose of the data processing (opt-in option).

The Act does not contain any special online privacy requirements other than those prescribed by the GDPR.

KEY CONTACTS

Karanovic & Nikolic
www.karanovic-nikolic.com/

Danijel Pribani
Senior Associate
T +385 1 5601 330
danijel.pribanic@karanovic-nikolic.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CYPRUS

Last modified 10 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Protection of Physical Persons Against the Processing of Personal Data and Free Movement of such Data Law 125(I)/2018, that implements certain provisions of the GDPR into local law, entered into force on July 31, 2018 (the "**Law**").

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal**

convictions and offences (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Bill uses the definitions provided under the GDPR without any derogation.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The authority designated under the Law as being the local regulatory body for the purposes of the GDPR is the Commissioner for the Protection of Personal Data in Cyprus (the "Commissioner").

The Law affords certain powers to and imposes obligations on the Commissioner which are in addition to the GDPR, including, inter alia, the following:

- Examination of complaints and providing information to the person making the complaint within 30 days of submission thereto.
- The obligation to inform the data subject, the data controller and the processor of the deadlines indicated under Articles 60-66 of the GDPR.
- The publication of a list of processing activities requiring the appointment of a data protection officer.
- To consult specialists or the police for exercising its regulatory powers under Article 58 of the GDPR.
- To enter, without giving any prior notice to the data controller or the processor or their representatives, any office, business premises or means of transport with the exception of housing premises, for inspections.
- To inform the Attorney General's Office and / or the police for breaches of the GDPR and the national law giving rise to criminal liability.
- To permit the combination of filing systems and to impose terms and conditions in relation thereto.
- To impose terms and conditions to the exemption from the obligation of the data controller to notify data subjects for breaches of personal data as provided for in Article 23 of the GDPR.

- To impose explicit restrictions on the transfer of special categories of personal data to third countries or international organizations.

Further, the Certification Body for the purposes of Article 43 of the GDPR is the Cyprus Organisation of the Promotion of Quality which is the national organization for accreditations in Cyprus operating under the Standardisation, Accreditation and Technical Notification Law (L156(I)/2002).

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

There is no registration applicable with the exception of what is referred to in the immediately succeeding paragraph for data protection officers.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and

- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

According to the Law, the Commissioner may draw up and make available to the public a list of the processing operations and / or other instances which shall deem necessary the designation of a data protection officer (the "DPO") by the data controller and the processor. A list of names of data controllers and processors who have designated a DPO may be published on the Commissioner's website provided the data controller and the processor wish to be included therein.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in

effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Collection and procession of genetic and biometric data for the purpose of health and life insurance is prohibited.

Subject to the above, where processing of genetic and biometric data is based on consent, subsequent and separate consents should be obtained for any further processing.

Further, according to the Law, impact assessment and prior consultation with the Commissioner are required in the following instances:

- when a combination of filing systems of public authorities or certification bodies, is conducted in relation to special categories of personal data or data relating to criminal offences or penalties or will be carried out on the basis of the use of an ID number or any other identifier of general application;
- where, subject to the provisions of Article 23 of the GDPR, measures are taken by the data controller to restrict the rights referred to under Article 12, 18, 19 and 20 of the GDPR;
- where the data controller is exempted from the obligation to notify data subjects for breaches of personal data for one or more of the purposes listed in Article 23(1) of the GDPR, including inter alia, national security, defense, public security, prevention, investigation, detection or prosecution of criminal offences etc;
- where national legislation or regulations issued pursuant thereto provide for a specific action or series of processing activities; and
- where special categories of personal data will be transferred in a third country or an international organization by the controller or the processor, on the basis of a derogation for specific situations provided for under Article 49 of the GDPR.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

With regards to transfer of special categories of personal data, prior to such data being transferred to a third country or an international organization on the basis of appropriate safeguards provided for under Article 46 of the GDPR or on the basis of binding corporate rules under Article 47 of the GDPR, the data controller or the processor needs to inform the Commissioner of its intention in transferring the said data. The Commissioner may impose express restrictions for such transfer.

Similarly, when special categories of personal data are to be transferred to a third country or an international organization on the basis of a derogation for specific situations provided for under Article 49 of the GDPR, the Commissioner may impose express restrictions for such transfer.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate,

context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

There are no derogations or additional requirements introduced by the Law in relation to security.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

According to the Law, the data controller may be exempted, in whole or in part, from his obligation to notify data subjects for breaches of personal data for one or more of the purposes listed in Article 23(1) of the GDPR, including inter alia, national security, defense, public security, prevention, investigation, detection or prosecution of criminal offences etc. In order for the foregoing to apply, an impact assessment and a prior consultation with the Commissioner need to be conducted. The Commissioner may also set out specific terms and conditions for such exemption.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

According to the Law, the Council of Ministers may, upon a recommendation of the Commissioner, issue regulatory administrative acts (secondary legislation) in order to effectively enforce the GDPR and applicable national law.

Further, with regards to Article 83 of the GDPR, the Law provides that the administrative sanction imposed in relation thereto shall not exceed EUR 200,000.

With regards to breaches of, inter alia, Articles 30, 31, 33, 34, 35, 42 and of Chapter V of the GDPR, the Bill provides that any such breach shall constitute a criminal offence which may result in the imposition of imprisonment up to three years and / or monetary fines up to EUR 30,000 (where the breach was due to negligence) or imprisonment up to five years and / or monetary fines up to EUR 50,000 (where the breach was intentional).

Where the data controller or processor is a company or a group of undertakings, then the person indicated as such in its article of association will be held liable for breaches of the GDPR and / or the national law. In case of public authorities or bodies, the head of such authority or the person who is effectively exercising the administration of such authority will be held liable for such breaches.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Regulation of Electronic Communications and Postal Services Law of 2004 (112(I)/2004) as amended (the "**Electronic Communications and Postal Services Law**") will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (*eg*, an email address is likely to be personal data for the purposes of the Electronic Communication and Postal Services Law).

Section 106 of the Electronic Communications and Postal Services Law states the following:

1. The use of automatic calling machines, fax, or electronic mail, or SMS messages, for the purposes of direct marketing, may only be allowed in respect to subscribers or users who have given their prior consent

2. Unsolicited communications for the purposes of direct marketing, by means other than those referred to in (1) above, are not allowed without the consent of the subscribers or users concerned

3. The rights referred to in (1) and (2) above shall apply to subscribers who are natural persons. The Commissioner of

Electronic Communications and Postal Regulation, may, after consultation with the Personal Data Commissioner, issue orders to safeguard that legitimate interests of legal persons, regarding unsolicited communications, are adequately protected. In 2005, the Commissioner of Electronic Communications and Postal Regulation issued the 2005 Order regarding Safeguarding the Interests of Legal Persons in relation to Unsolicited Communications, by virtue of which the protection from unsolicited communications for the purposes of direct marketing has been extended to legal persons as well

4. Notwithstanding (1) above, in cases where a natural or legal person obtains from its customers contact details for electronic mail, in the context of the sale of a product or a service, the same natural or legal person may use these electronic details for direct marketing of its own similar products or services, provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of their electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use, and

5. Electronic mail sent for direct marketing must not disguise or conceal the identity of the sender or the person on whose behalf and / or for the benefit of the communication is made, or without a valid address to which the recipient may send a request that such communication cease.

ONLINE PRIVACY

Part 14 of the Electronic Communications and Postal Services Law deals with the collection of location and traffic data and use of cookies (and similar technologies) by publically available electronic communication service providers.

Traffic Data

Traffic Data concerning subscribers and users, which are submitted to processing so as to establish communications and which are stored by persons, shall be erased or made anonymous at the end of a call, except:

- for the purpose of subscriber billing and interconnection payments, and

- if the subscriber or user consent that the data may be processed from a person for the purpose of commercial promotion of the services of electronic communications of the latter or for the provision of added value services. Users or subscribers have the possibility to withdraw their consent for the processing of Traffic Data at any time.

The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information. Users or subscribers shall be given the possibility to withdraw their consent for the processing of Traffic Data at any time.

Location Data

Location Data may only be processed when made anonymous, or with the explicit consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.

The service provider must inform the users or subscribers, prior to obtaining their consent, of the following:

- type of Location Data which will be processed

- the purpose and duration of the processing, and

- whether the data will be transmitted to a third party for the purpose of providing the value added service.

Users or subscribers shall be given the possibility to withdraw their consent for the processing of Location Data at any time.

Cookie Compliance

The storage and use of cookies and similar technologies is permitted only if the subscriber or user concerned has been provided with clear and comprehensive information, inter alia, about the purposes of the processing, and has given his consent in accordance with the Processing of Personal Data Law.

The above shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

With regards to information society services, when such services are addressed to a child and provided to him / her on the basis of his / her consent – such consent is valid if he / she is at least 14 years old.

KEY CONTACTS

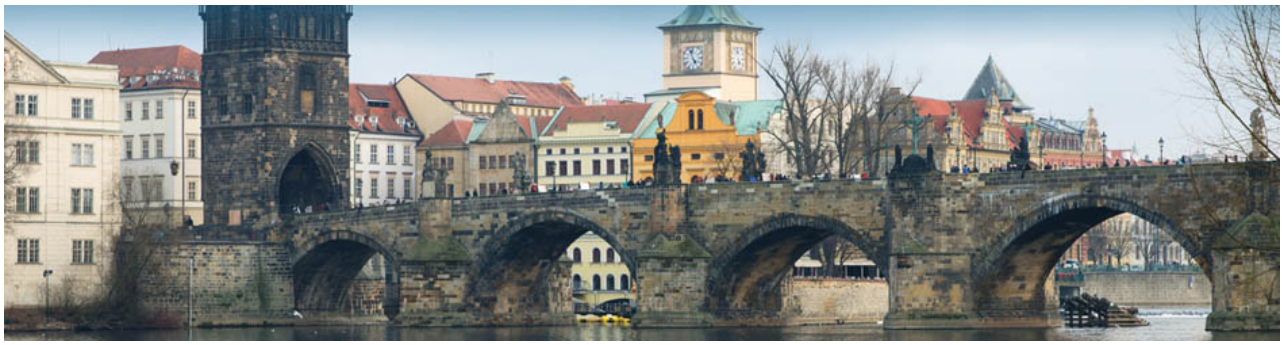
Pamboridis LLC
www.pamboridis.com/

Christy Spyrou
Partner
T +357 22 752525
spyrou@pamboridis.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CZECH REPUBLIC



Last modified 20 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The GDPR implementation law has been recently adopted by the lower chamber of the Czech Parliament (the approved consolidated version reflecting last-minute amendments resulting from motions of individual deputies is not yet available at the time of this update) and will now proceed to the Senate.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger

corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organisations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited

to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the

data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU - U.S. Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;

b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation's data protection officer or other contact, the likely consequences of the

breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to

receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.

- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

When dealing with e-marketing, it is necessary to bear in mind that it is quite strictly regulated in terms of Act No. 480/2004 Col. on Certain Services of Information Society ("CSIS") as well as other previously mentioned regulations (esp. the Data Protection Directive and the Act).

CSIS states that before sending an e-mail containing marketing information, the consent of the receiver must be obtained (so called "opt-in" principle). In some cases, such as e-marketing sent to existing customers of the sender, the consent of the customer is implied until it is withdrawn (so called "opt-out" principle). Furthermore, each such message must contain clear and visible information that any further sending of such e-mails can be rejected by the receiver together with the sender's contact information and information on whose behalf the e-mail is being sent. Last but not least, each such e-mail must be clearly tagged as a commercial message.

In order to maintain e-marketing as an effective tool, its sender should operate with good-quality databases, which enable a direct targeting of the relevant message. The sender should ensure, in particular, that (i) he will duly obtain the right to use the database for e-marketing purposes and also that (ii) personal data in the database were lawfully obtained and can be lawfully disposed of by the database owner.

When processing personal data for marketing databases, it is necessary to abide strictly by the Act. All rules described above apply to e-marketing respectively.

ONLINE PRIVACY

Online privacy is also supervised by the Office. Handling personal data is subject to the similar rules as mentioned above and specific issues are governed by Act No. 127/2005 Coll. on Electronic Communications ('AEC').

Consent to collection and processing of personal data may be expressed by electronic means, especially by filling in an electronic form.

Public electronic communication service providers are obliged to ensure the security of the personal data they process which includes technical security and creation of internal organisational regulations.

In cases of a personal data breach a public electronic communication service provider is obliged to notify the Office "without necessary delay", and in the event that the breach of protection could very significantly affect the privacy of a certain individual, such person must be notified as well.

Apart from a few exceptions, traffic data held by a public electronic communication service provider must be erased or anonymised when it is no longer necessary for the transmission of a communication.

As regards cookies, the Czech law is still using the 'opt-out' principle because the user must be informed and explicitly allowed to refuse the cookies storage (no prior consent required). The 'opt-in' principle as introduced by the Directive 2009/136/EC has not been implemented into Czech law, although many state authorities, including the Office, publicly declared the opposite. Nevertheless, due to the above-mentioned ambiguity, we cannot exclude the risk that the Office will require the prior consent to be given by visitors of the relevant web-site according to the generally applicable obligation under the Act, if the relevant cookie is able to identify the specific user.

Relevant supervising and enforcing authorities in this area are primarily the Office and to some extent also the Czech Telecommunication Office.

KEY CONTACTS

Jan Rataj
Senior Associate
T T +420 222 817 800
jan.rataj@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

DENMARK

Last modified 10 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

To implement the GDPR, the Danish Parliament enacted the Danish Act on Data Protection (the 'Danish Data Protection Act') on May 17, 2018, enforceable on May 25, 2018 and replacing the previous Danish Act on Processing of Personal Data (Act no. 429 of 31/05/2000). Hence, data protection and processing in Denmark is now regulated by the GDPR as supplemented by the Danish Data Protection Act.

The Danish Data Protection Act does not apply to Greenland and the Faroe Islands.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions used in the Danish Data Protection Act correspond to the definitions as set out in the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Datatilsynet ('DPA')
Borgergade 28, 5
DK 1300 København K

T +45 3319 3200
F +45 3319 3218

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

In Denmark, the following types of processing require the DPA's preapproval:

- private data controllers' processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation ('Special Categories of Personal Data'), solely in the public's interest
- transfer of Special Categories of Personal Data, originally processed for scientific and statistic purposes, if i) such data is to be processed outside the geographical scope of the GDPR, ii) the data constitutes biometric data or iii) if the data is to be published in a well-known paper
- processing personal data in a register on behalf of a private data controller:
    - solely for the purpose of warning other businesses from engaging in business with or employing a natural person
    - with the intention of commercial exploitation of data on the natural person's creditworthiness and financial solidity, or
    - for the creation of a register on judicial information

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;

- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

Under the Regulation, organizations shall designate a data protection officer ('DPO') in any case where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity
- the core activities of the data controller or the processor consist of processing operations which, by their nature, their scope and / or their purposes, require regular and systematic monitoring of data subjects on a large scale, or
- the core activities of the controller or the processor consist of processing on a large scale of Special Categories of Personal Data and personal data relating to criminal convictions and offences

The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks referred to in the GDPR.

Under the Danish Data Protection Act, the DPO is subject to a duty of secrecy and is prohibited against transfer and exploiting any personal data processed in their capacity of being DPO.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);

- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are

processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's

highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The GDPR differentiates between 1) Personal data, 2) Special Categories of Personal Data, 3) Data on criminal offences and 4) Civil registration numbers. See below.

1. Personal data

Under the GDPR, data controllers may legally register and process personal data (all data except the Special Categories of Personal Data, Data on criminal offences and civil registration numbers) when at least any of the following conditions are met:

- the data subject has given his explicit consent in accordance with article 7 and 8 (children's consent) of the GDPR
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- processing is necessary for compliance with a legal obligation to which the controller is subject

- processing is necessary in order to protect the vital interests of the data subject or any other natural person
- processing is necessary for the performance of a task carried out in the public interest or for the performance of a task carried out in the exercise of official authority vested in the data controller, or
- processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third-party to whom the data is disclosed, unless these interests are overridden by either the data subject's fundamental rights including its civil rights or other interests of the data subject

Under the Danish Data Protection Act, it is legal to process data on children with a minimum age of 13. Data on children younger than 13 years old is only legal if the child's parents or legal guardians have given their explicit consent.

2. Special Categories of Personal Data

Special Categories of Personal Data (as detailed under 'Registration') may be processed only when at least any of the following conditions are met:

- the data subject has given his explicit consent to the processing of such data for one or several purposes
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment and other specific rights such as social security and social protection law
- processing is necessary to protect the vital interests of the data subject or of another natural person where the person concerned is physically or legally incapable of giving his or her consent
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects
- processing relates to personal data which are manifestly made public by the data subject
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity, or
- processing is necessary for reasons of substantial public interest. The DPA must approve the processing unless such is carried out by a public organization.

Personal data and Special Categories of Personal Data may be processed, if such process is carried out in relation to the data subject's employment at the data controller, if such process is necessary for the data controller to comply with employment-related obligations or rights under applicable law or collective agreements, or if the process is necessary for the data controller or third-party's possibility to pursue legitimate interests originating from other legislation or collective agreements as long as the civil rights and interests of the data subject precedes.

3. Data relating to criminal convictions and offences

Data relating to criminal convictions and offences may be processed by public data controllers only if the processing is strictly necessary for the performance of regulatory and public tasks. No such data can, however, be passed on, unless at least any of the following conditions are met:

- the data subject concerned has given his or her explicit consent in accordance with article 7 in the GDPR; or
- the pass on is performed to attend private or public interests, significantly overriding consideration of non-disclosure and the data subject's interests in general; or
- the pass on is necessary for the performance of regulatory and public business or for a public authority to decide on a ruling; or
- the pass on is necessary for the performance of either a natural person or a company's tasks on behalf of public authorities.

Private data controllers may process data relating to criminal convictions and offences, if the data subject in question has given his or her explicit consent in accordance with article 7 of the GDPR, or if the processing is strictly necessary to

carry out interests significantly exceeding the interests of the data subject. None of the data may be passed on without the explicit consent of the data subject, unless such pass on is performed in the interests of either the public or private data controller or the data subject in question on the condition that that these interests significantly exceed the consideration of non-disclosure.

Both public and private actors may process data relating to criminal convictions and offences if at least one the following conditions is met:

- processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment and other specific rights such as social security and social protection law
- processing is necessary to protect the vital interests of the data subject or of another natural person where the person concerned is physically or legally incapable of giving his or her consent
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects
- processing relates to personal data which are manifestly made public by the data subject
- processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity, or
- processing is necessary for reasons of substantial public interest. The DPA must approve the processing unless such is carried out by the public organization.

4. Civil registration numbers

Civil registration numbers (in Danish and henceforth 'CPR-no.') may be processed by public organizations for the purpose of identification or as reference number.

Private data controllers may process CPR-no. when at least one of the following conditions are met:

- the process is required under statutory law
- the data subject concerned has given his or her explicit consent in accordance with article 7 of the GDPR
- the processing is carried out for scientific or statistic purposes (however not for publication which requires a specific consent)
- the CPR-no. is passed on as part of the company's natural operations and such pass on is of significant importance to the company to ensure identification of the data subject in question or requested by a public authority
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment and other specific rights such as social security and social protection law
- processing is necessary to protect the vital interests of the data subject or of another natural person where the person concerned is physically or legally incapable of giving his or her consent
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects
- processing relates to personal data which are manifestly made public by the data subject
- processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity, or
- processing is necessary for reasons of substantial public interest. The DPA must approve the processing unless it is carried out by a public data controller

The data controller must, at the time when personal data are obtained (no later than within one month after), provide the

data subject with the necessary information to fulfil the duty of information, including information about:

- the identity of the data controller, his representative and the DPO (if applicable)
- the contact details of the data controller/the representative
- the categories of data concerned
- the purposes of the processing for which the data is intended as well as the legal basis for the processing
- the legal basis for the process in details
- the recipients or categories of recipients of the personal data, (if any)
- (where applicable), information of transfer of data or the intention hereof
- The period for which the data will be stored
- The data subject's rights, including to lodge a complaint, deletion, insight and correction
- From which source the personal data originate (if applicable), and whether it came from publicly accessible sources (if applicable)

Under the Danish Data Protection Act the above-mentioned obligation does not apply if interests of the public, other people, or the data subject itself, exceeds the data subject's interest in obtaining the information.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Danish Data Protection Act does not regulate transfer of personal data. Thus, the article of the GDPR applies, under which data controllers may transfer all types of personal data to a third country or an international organization out of the EU/EEA if any of the following conditions are met:

- the EU Commission has established that the third-country/area or one or more specific sectors in the third country, or the international organization has adequate safeguards with respect to the protection of the rights of the data subject
- the controller or processor has provided appropriate safeguards, on the condition that enforceable data subject rights and effective legal remedies for data subjects are available (such as through binding corporate rules – approved by the DPA)
- the data controller or data processor and the international organization enter into the standard terms approved by the EU Commission

If no approval has been obtained on the third country's adequate safeguards and no appropriate safeguards have been provided including binding corporate rules, personal data can be transferred to a third country or an international organization if one of the following criteria are met:

- the data subject has given his explicit consent
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party
- the transfer is necessary or legally required on important public interest grounds
- the transfer is necessary for the establishment, exercise or defence of legal claims
- the transfer is necessary in order to protect the vital interests of the data subject or other natural person, where the person concerned is physically or legally incapable of giving his or her consent
- the transfer is made from a register which according to law or regulations is open to consultation either by the public in general or by any person who can demonstrate legitimate interests, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The Danish Data Protection Act does not set out provisions on security requirements. Thus, the articles of the GDPR apply, under which data controllers and data processors must implement appropriate technical and organizational security measures necessary to protect data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in the Danish Data Protection Act.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Danish Data Protection Act does not set out provisions on notification in case of security breach. Thus, the articles of the GDPR apply, under which the data must notify the DPA no later than 72 hours after becoming aware of the security breach.

Breaches can be reported to the Danish Data Protection Agency by filling out a form on the Danish Business Authority's website.

Further, if the security breach is likely to expose the data subject to risk related to its rights and civil rights, the data controller shall notify the data subject without unnecessary delay.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be

scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The DPA, which consists of a Council and a Secretary, is responsible for the supervision of all processing operations covered by the Danish Data Protection Act.

The DPA can request any information provided necessary for the DPA's operations including decision-making on whether the Danish Data Protection Act and the GDPR apply or not.

The DPA and its personnel can without a court order request access to premises from which processing of personal data is performed.

The DPA's decisions are final and not subject to recourse.

The DPA may investigate data processing occurring in Denmark and the legality thereof, despite the processing being subject to foreign law.

The DPA may publish its findings and decisions.

Any person suffering material or nonmaterial damage due to non-legal data processing can claim damages.

Unless a higher penalty is impeded, processing deemed unlawful under the Danish Data Protection Act, is sanctioned with a fine or prison for up to six months.

In general, the GDPR aims to sanction with fines which are effective, reasonable and have preventive effect. More specific, certain violations can be sanctioned with a fine of a maximum of EUR 10,000,000 or 2% of the total annual turnover (if a company). Other types of violations can be sanctioned with a fine of a maximum of EUR 20,000,000 or 4% of the total annual turnover (if a company).

The statute of limitation period is five years.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg,* an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

In general, unsolicited electronic marketing requires prior opt-in consent. The opt-in requirement is waived under the 'same service / product' exemption. The exemption concerns marketing emails related to the same products / services as previously purchased from the sender by the user provided that:

- the user has been informed of the right to opt out prior to the first marketing email
- the user did not opt out, and
- the user is informed of the right to opt out of any marketing email received. The exemption applies to electronic communication such as electronic text messages and email but does not apply with respect to communications sent by fax.

Direct marketing emails must not disguise or conceal the identity of the sender.

The GDPR applies to electronic marketing activities involving usage of personal data (*eg,* an email address which includes

the recipient's name).

Under the GDPR companies cannot pass on personal data to another company for direct marketing purposes or use the data on behalf of a company for marketing purposes, unless the data subject has given his or her explicit consent. In this regard, the strict standard for consent under the GDPR must be noted, and marketing consent forms must include a clearly worded opt-in mechanism (such as a ticking of an unticked consent box, or the signing of a statement, and *not* merely an acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

General customer information (general information forming the basis for customer classification) can, however, be passed on and processed without the data subject's consent, if such is necessary for the purposes of legitimate interests pursued by the company and these interests are not overridden by the interests of the consumer. However, Special Categories of Personal Data and CPR-numbers can only be processed for marketing purposes by the consent of the data subject.

The company passing on the personal data or processing the personal data on behalf of a company for marketing purposes, must prior hereto ensure that the data subject has not declined receiving marketing material by registering as such in the Danish Central Office of Personal Registration.

Particularly for controllers selling catalogs of data on natural persons or addressing these natural persons on behalf of a company it applies that only the natural person's name, work position, address, occupation, email, phone- and fax number and business information published in business registers can be processed. Any other kind of data can only be processed, if the data subject has consented thereto.

Further, specific rules on electronic marketing (including circumstances in which consent must be obtained) are regulated in Directive 2009/136/EC (the ePrivacy Directive), as transposed into the local laws of each Member State. In Denmark, the ePrivacy Directive has among other things been implemented in the Danish Marketing Practices Act.

Under the Danish Marketing Practices Act, a trader must not approach anyone by means of electronic mail, an automated calling system or a facsimile machine (fax) for the purposes of direct marketing unless the natural person concerned has given his prior consent. The trader must allow free and easy revocation of the consent.

Notwithstanding the above, a trader that has received a customer's electronic contact details in connection with the sale of products may market similar products to that customer by electronic mail, provided that the trader has clearly and distinctly given the customer the opportunity, free of charge and in an easy manner, of declining this both when giving his contact details to the trader and in all subsequent communications.

The ePrivacy Directive is to be replaced by the ePrivacy Regulation, a change which was forecast for spring 2018, however, now postponed indefinitely. From the wording of the latest draft, we can expect a significant toughening of the online and direct marketing landscape and, predictably, a convergence with the provisions in the GDPR.

ONLINE PRIVACY

Traffic data

Traffic data qualifies as personal data. Providers of telecommunication services may collect and use the following traffic data to the following extent:

- the number or other identification of the lines in question or of the terminal
- authorization codes, additionally the card number when customer cards are used
- location data when mobile handsets are used
- the beginning and end of the connection, indicated by date and time and, where relevant to the charges, the volume of data transmitted
- the telecommunications service used by the user
- the termination points of fixed connections, the beginning and end of their use, indicated by date and time and, where relevant to the charges, the volume of data transmitted, and

- any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes.

Stored traffic data may be used after the termination of a connection only where required to set up a further connection, for billing purposes or where the user has requested a connection overview.

The service provider may collect and use the customer data and traffic data of subscribers and users in order to detect, locate and eliminate faults and malfunctions in telecommunications systems. This applies also to faults that can lead to a limitation of availability of information and communications systems or that can lead to an unauthorized access of telecommunications and data processing systems of the users.

Otherwise, traffic data must be erased by the service provider without undue delay following termination of the connection.

Service providers have to inform the users immediately, if any faults of data procession systems of the users become known. Furthermore the service provider has to inform the users about measures for detecting and rectifying faults.

Location Data

Location Data qualifies as personal data. This data may only be processed as required for the provision of requested services and is subject to prior information of the user. For all other purposes, the user's informed consent must be obtained. According to Section 4a BDSG, 13 German Telemedia Act (TMG) this means that:

- the user's consent must be intentional, informed and clear. For this purpose the user must be informed on the type, the scope, the location and the purpose of data collection, processing and use including any forwarding of data to third parties
- the user's consent must be recorded properly
- the user must be able to access the content of his consent declaration any time. It is sufficient that such information is provided upon the user's request
- the user's consent must be revocable at all times with effect for the future.

Users must always be informed of the use of cookies in a privacy notice. Cookies may generally be used if they are required in order to perform the services requested by the user. Otherwise, users must be provided with an opt-out mechanism. For this purpose, information on the use of cookies together with a link on how to adjust browser settings in order to prevent future use is sufficient.

Germany has not yet taken any measures to implement the e-privacy directive. However, in February 2014 the German Federal Ministry of Economic declared that the European Commission considers the Cookie Directive as implemented in Germany. However, since the European Commission´s exact interpretation is not known, a final official clarification is awaited. It therefore remains to be seen whether an active opt-in, *eg,* by clicking on a pop-up screen will be required in the future.

Different rules apply in the case of tracking technologies which collect and store a user's IP address. Since IP addresses qualify as personal data, their processing for tracking and marketing services requires active opt-in consent.

Directive 2009/136/EC (the ePrivacy Directive) was among other things also implemented in the Danish Act on Electronic Communications Services and Networks which came into force on May 25, 2011 in accordance with the implementation deadline in the Directive. In accordance with this act, the Danish Parliament adopted the Danish Executive Order on Electronic Communications Services and Networks which came into force on May 25, 2018 (the 'Cookie Order').

The Cookie Order should be read in the light of GDPR, where the rules regulate collection of data in a broader sense, not considering whether such information may be used to identify a natural person.

Under the 'Cookie Order' the use of cookies requires a consent. The consent must be freely given and specific. However, this does not imply that consent must be obtained each time a cookie is used but a user must be given an option. The consent must be informed which implies that a user must receive information about the consequences of consenting. Finally, the consent must be an informed indication of the user's wishes.

Normally, consent is obtained through tick-the-box but also the use of a homepage after having received the relevant information concerning cookies can constitute consent. Yet consent by use of a homepage must be used with caution.

In addition to this, the information to the user must fulfill the below mentioned requirements:

- the information must be clear and easy to understand
- the purpose of the use of the cookies must be provided
- the identity of the person or entity which is responsible for the use of the cookies must appear
- the possibility of withdrawal of consent must be easily accessible and be described in the information, and
- this information must be easily accessible for the user at all times

The ePrivacy Directive is to be replaced by the ePrivacy Regulation, a change which was forecast for spring 2018, which has now, however, been postponed indefinitely. The timeframe for changes to abovementioned rules are thus currently unknown.

From the wording of the latest draft, however, it is unsurprisingly safe to say that the definition of consent used in the GDPR is carried across into the draft ePrivacy Regulation text. Further, the draft also introduces significant practical changes, so that obtaining consent will require much more effort. Technology providers are required to include default settings which must all be set to preclude third parties from storing information on, or using information about, an end-user's device. So, browsers would have to be pre-configured so that cookies used for frequency capping of ads or ad-serving would be blocked by default unless a user opts to enable them.

KEY CONTACTS

Marlene Winther Plas
Partner
T +45 33 34 00 47
marlene.plas@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

DOMINICAN REPUBLIC

Last modified 28 January 2019

LAW

Section 44 of the Dominican Constitution recognizes citizens' right to access their personal data stored in public or private databases, as well as their right to information concerning the purpose and use of the same.

The Constitution also establishes that the processing of personal data must be carried out in accordance to the principles of:

- Reliability
- Legality
- Integrity
- Security, and
- Purpose of the information

The collection, storage and safekeeping of personal data, as well as usage and access rights concerning such personal data, are governed by the provisions of Law No. 172-13 on the Protection of Personal Data enacted December 13, 2013 (DPL).

In addition to setting forth the legal regime for the protection of personal data, the DPL establishes regulations governing the constitution and operation of credit bureaus.

For the purposes of the DPL, the term '*credit bureau*' refers to companies dedicated to collecting, organizing, storing, conserving, providing, transferring or transmitting data regarding consumers (including goods and services related to the same), as well as any other information provided by the Superintendent of Banks.

DEFINITIONS

Definition of personal data

Personal data consists of any information, whether numerical, alphabetical, graphic, photographic, or acoustic, or any other type of data which concerns individuals that are identified or identifiable.

Definition of sensitive personal data

The term 'sensitive data' refers to personal data that reveals its subject´s:

- Political opinions
- Religious, philosophical or moral convictions
- Affiliation to labor unions, and
- Information concerning health or sex life

Personal data concerning the health of an individual encompasses any information concerning their past, present or future physical

or mental health.

NATIONAL DATA PROTECTION AUTHORITY

The Dominican Republic does not have a national data protection authority.

Section 29 of the DPL establishes that databases and registries, whether public or private, intended to provide credit reports (ie credit bureaus) are subject to the inspection and supervision of the Superintendent of Banks.

REGISTRATION

Except for credit bureaus, the Dominican Republic does not maintain a registration of personal data controllers or databases, nor of companies that carry out the processing of personal data.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer under the DPL.

COLLECTION & PROCESSING

The general rule for the treatment of personal data under the DPL is the consent requirement. Consent is valid when there is a manifestation of free will, in an unequivocal, specific and informed manner, whereby the data subject consents to the treatment of personal data concerning him or her.

The DPL provides that the treatment and transfer of personal data is illegal when the data has not consented to such usage, unless an exception is provided by law.

For purposes of the foregoing, the DPL defines treatment as operations and procedures (electronic or otherwise), that allow for the:

- Collection
- Storage
- Organization
- Modification
- Evaluation
- Destruction
- In general, the processing of personal data, or
- Its transfer to third parties via communications, interconnections or transfers

Exceptions to the consent requirement include, among others:

- When the data is obtained from a public source
- When the data is obtained for the exercise of public duties or pursuant to a legal obligation to do so
- When the data is obtained for marketing purposes and is limited to certain basic information (*eg*, name, ID, passport, tax ID)
- The data derives from a commercial, employment or contractual relationship, or from a professional or scientific relationship with the data subject, and is necessary for its development or compliance

TRANSFER

Transfer is considered a form of 'treatment' of personal data under the DPL; hence, the rules apply, including consent requirements. Additional restrictions are provided under the DPL for international data transfers.

Personal data may only be transferred internationally if the owner of the data expressly authorizes such transfer, or if such transfer is necessary for the performance of a contract between the owner of the data and the person or entity responsible for the treatment of the personal data.

SECURITY

The controller and, if applicable, the processor, is required to adopt and implement the necessary technical, organizational and security measures to safeguard personal data and avoid its:

- Alteration
- Loss
- Treatment
- Consultation, or
- Unauthorized access

The DPL prohibits the storage of personal data in files, records or databases that do not meet the necessary technical conditions for guaranteeing their integrity and security. Additionally, credit bureaus and users or subscribers shall take the necessary measures to prevent the alteration, loss or unauthorized access to personal data.

BREACH NOTIFICATION

There is no obligation to notify a breach.

ENFORCEMENT

Data subjects have the right to institute *habeas data* proceedings to obtain information about the data held that refers to the relevant data subject.

The DPL expressly recognizes the right of data subjects to recover damages for violations of their right to privacy and the integrity of their personal data. Additionally, the DPL provides criminal sanctions (including fines and imprisonment ranging from six months to two years) which may result from violating the DPL.

Law No. 310-14 Which Prohibits the Sending of Commercial Unsolicited Messages (SPAM), enacted on August 8, 2014 ('SPAM Law No. 310- 14',) also provides criminal sanctions for fraudulently obtaining personal data from public websites for commercial purposes (including imprisonment ranging from six months to five years, and fines from 1 to 200 times the minimum wage).

ELECTRONIC MARKETING

Sending commercial or promotional communications via electronic mail is regulated by SPAM Law 310-14. Law 310-14 requires the consent of the recipient in order to deliver commercial communications, unless an exception to said consent requirement is expressly provided by law.

Law 310-14 provides that:

- The word 'Publicity' (*Publicidad*) must be included in the subject field of the email
- Commercial communications must include an email address or other similar mechanism which allows the recipient to send a message indicating their desire to stop receiving such communications (opt-out)

ONLINE PRIVACY

The Dominican Republic has not enacted specific legislation governing online privacy or the use of 'cookies', although the provisions of the DPL concerning data protection would apply.

Additionally, the unauthorized use of 'cookies' could implicate computer misuse laws prohibiting unauthorized access to computers and information therein, particularly those contained in Law No. 53-07 on high-tech crimes and felonies.

KEY CONTACTS

Mary Fernandez
Partner
Headrick
T +809 473 4500
mfernandez@headrick.com.do

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

EGYPT

Last modified 26 January 2017

LAW

Egypt does not have a law which regulates protection of personal data. However, there are some piecemeal provisions in connection with data protection in different laws and regulations in Egypt. Further, a draft law regulating the freedom of data exchange and data protection was drafted, but it has not yet been approved or published. It is expected to be discussed before the Egyptian parliament.

Constitutional principles concerning individuals' right to privacy under the Egyptian Constitution as well as general principles on compensation for unlawful acts under the Egyptian Civil Code govern the collection, use and processing of personal data.

In addition, the Egyptian Penal Code no. 58/1937 imposes criminal punishment for unlawful collection of images or recordings for individuals in private places. Some other laws provide for protection and confidentiality on certain data, such as the Egyptian Labour Law no. 12/2003 (confidentiality of the employee's file information including punishment and assessment) and the Egyptian Banking Law no. 88/2003 (confidentiality of client and account information). Egyptian Civil Status Law no. 143/1994 provides for the confidentiality of citizens' civil status data. The Executive Regulations of Mortgage Finance Law no. 148/2001 issued by virtue of Cabinet Decree no. 1/2001 as amended by Prime Minister Decree no. 465/2005 has a similar clause which provides for the confidentiality of the data of the clients of mortgage finance companies. The Egyptian Telecommunications Law no. 10/2003 provides for the privacy of telecommunications and imposes penalties which account to imprisonment in some cases on the unauthorized violation of such privacy. Egyptian Penal Code no. 58/1937 and Physicians Code of Ethics provide for the privacy of the patient's information and prohibition to disclose it without the patient's prior consent. The violation of such prohibition could be penalized by imprisonment and/or minimal fines.

Article 57 of the Egyptian Constitution promulgated in January 2014 provides for the protection of privacy and secrecy of, inter alia, mails, phone conversations and other methods of communication. The aforementioned shall not be monitored, inspected or confiscated unless by virtue of a prior court order and for a limited period of time as regulated by the law.

The Egyptian Constitution has not defined data protection. However, it refers to the legislative authority to regulate the communication of data in a manner that does not encroach upon the privacy of citizens, their rights and National Security.

DEFINITIONS

Definition of personal data

There is no definition of personal data or private life under Egyptian law or the Constitution. However, Egyptian laws provide examples of the personal data that are protected such as the Labour Law. Article 77 of the Labour Law provides that the employees' files that must be kept by the employer (as mentioned below) includes the employee's personal data such as his name, job, professional skills when he joined the workplace, domicile, marital status, salary, starting date of his work, the holiday leave he takes, punishments imposed on him and the reports of his superiors on his work.

Definition of sensitive personal data

There is no definition of sensitive personal data under Egyptian law.

NATIONAL DATA PROTECTION AUTHORITY

There is no national authority responsible for data protection in Egypt.

REGISTRATION

There is no requirement or facility to register data in a specific register.

DATA PROTECTION OFFICERS

There is no requirement in Egypt for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

According to the principles of the Egyptian Civil Code, the collection, use or processing of personal data is prohibited in case it violates the individual right to privacy and provided that such collection, use or processing constitutes a fault pursuant to the Egyptian Civil Code. A fault is defined by the judiciary as an act or omission that violates an obligation imposed by the law or assumed caution and care of the average man.

Only data which is considered pertinent to the data subject's private life requires the consent of the data subject. The competent courts will determine whether specific data is considered pertinent to the private life of the data subject or not and whether the collection or processing of such data violates an obligation imposed by the law or assumed caution and care of the average man.

Collecting data about the employee is required by law (Article 77 of the Egyptian Labour Law) which provides that each employer must keep a file for each employee which includes their personal data. Only certain persons are authorised by the law to have access to such data.

TRANSFER

The same general principles applicable to data collection and processing mentioned above apply to the transfer of data. The data controller may not transfer data pertinent to the private life of the data subject except after obtaining the consent of the data subject, unless otherwise permitted by the law.

SECURITY

Other than client and account data in banks, personal data controllers are not required by law to take specific measures against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data. The data controllers will be held liable according to the average man standard if their acts or omissions cause the processing, loss, destruction or damage to such personal data and this in turn results in damage being caused to the data subject.

BREACH NOTIFICATION

There is no mandatory legal requirement in the Egyptian law to report data security breaches or losses to the authorities or to data subjects.

ENFORCEMENT

As a general rule, civil liability may be raised in connection with violations against the individuals' right to privacy. The prejudiced data subject should establish to the competent court the unlawful act, the damage occurred to them and the causation relationship between the unlawful act and the damage. Compensation is calculated on an 'actual damages' basis and is not punitive. Moral damages are also compensated.

Civil liability for data privacy infringement has not been frequently claimed before Egyptian courts.

ELECTRONIC MARKETING

Egyptian law does not have any specific provisions which regulate Electronic Marketing.

ONLINE PRIVACY

The Egyptian Constitution issued in 2014 provides that internet security is considered an essential part of the economic institution and national security and that the state is responsible for taking any required measures to maintain said security as regulated by the law. However, Egyptian law does not have any specific provisions which regulate online privacy.

There are number of draft legislations that are expected to be promulgated by Parliament in the coming period on state surveillance and the transfer and processing of data, including (i) draft law regarding the combat of the electronic and information crimes; and (ii) draft law regarding cyber security.

Also, please note that the Egyptian Computer Emergency Response Team, which is affiliated to the Ministry of Communication and Information Technology, has been established since April 2009 and is responsible for, inter alia, providing support to entities, banking and government sectors to tackle cyber security threats.

Further, Article 64 of the Telecommunication Law no. 10/2003 provides that the services provider or processor of telecommunications services must maintain, at its sole expense, all the technical capability which will allow the armed forces and the national security authorities to perform its competences within the limit of the law, without prejudice to the protection of private life of the individuals. This provision might be interpreted by the authorities to give them the right to have access to or surveillance on the data and information transferred or processed through telecommunication services in Egypt.

KEY CONTACTS

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ESTONIA

Last modified 10 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

In Estonia, all derogations / additional requirements to the GDPR are provided in the new Personal Data Protection Act (PDPA) and the Personal Data Protection Implementation Act (Implementation Act). Separately, amendments to the Penal Code have been proposed to allow for the fine amounts as envisioned under the GDPR to be imposed in Estonia.

The new PDPA was adopted by the Estonian parliament on December 12, 2018. It will enter into force on January 15, 2019.

The draft Implementation Act and amendments to the Penal Code are currently undergoing parliamentary debate. The Implementation Act will likely be adopted in the beginning of 2019.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location

data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The PDPA and the Implementation Act use the same definitions as the GDPR and do not foresee any new terms or terms defined differently from the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The PDPA specifies that in the meaning of article 51(1) of the GDPR the independent supervisory authority of Estonia shall be the Estonian Data Protection Inspectorate (DPI). The PDPA further specifies the requirements for and appointing of the head of the DPI.

In addition to the tasks provided in Article 57 of the GDPR, the PDPA specifies that the DPI is competent to:

- raise awareness and understanding of the public, the controllers and processors about the risks of processing personal data, the standards and safeguards applicable to processing, and the rights related to the processing of personal data; The DPI may provide indicative guidance for this task;
- provide information to the data subject, upon request, about the exercise of his rights under this PDPI and, if necessary, cooperate with other supervisory authorities of the European Union Member States for this purpose;
- initiate, where necessary, misdemeanor proceedings and impose sanctions in the event where it is not possible to

achieve compliance with the requirements provided by law or GDPR with the application of other administrative measures;
- cooperate with international data protection supervisory organizations and other data protection supervisory authorities and other competent authorities and persons of foreign states;
- monitor relevant trends insofar as they affect the protection of personal data, in particular the development of information and communication technology;
- participate in the European Data Protection Board;
- apply administrative coercion to the extent and pursuant to the procedure prescribed by law;
- submit opinions to the Estonian parliament, the Government of the Republic, the Chancellor of Justice and other institutions and the public on its own initiative or upon request on issues related to the protection of personal data;
- perform other duties arising from law.

In addition to the rights and powers under the GDPR the PDPA specifies that the DPI has the right to:

- warn the controller and the processor that the data processing activities are likely to violate the PDPA;
- demand the rectification of personal data;
- demand the deletion of personal data;
- demand restriction of processing of personal data;
- demand the termination of the processing of personal data, including destruction or archiving;
- implement organizational, physical and informational security measures for the protection of personal data without delay, if necessary, in accordance with the procedure provided for by the Substitutive Enforcement and Penalty Payment Act, if necessary, in order to prevent damage to the rights and freedoms of a person, unless personal data are processed by a public authority;
- impose a temporary or permanent restriction on the processing of personal data, including a prohibition on the processing of personal data;
- initiate state supervisory proceedings on the basis of a complaint or on its own initiative.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Given that the GDPR does not provide for the registration of processing personal data, registries and systems will no longer exist. Pre-recorded data will remain as archived information about past activities.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;

- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

In relation to DPOs, the PDPA and the Implementation Act do not foresee any derogations / additional requirements to the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record- keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the

controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

- Processing after data subject's death. According to the PDPA the consent of the data subject is valid during the data subjects life and 10 years after the data subject's death, unless otherwise provided by the data subject. If the data subject has died underaged, the data subject's consent shall be valid for 20 years after his / her death. After the data subject's death, the processing of his/her personal data is permissible upon the consent of one of the heirs of the data subject, unless:
    - 10 years have passed from the death of the data subject;

- More than 20 years have passed from the death of an underaged data subject
- Another legal basis for processing exists.

The aforementioned consent is not required when the processing includes only the data subject's name, gender, time of birth and death, the fact of death, and the time and place of burial.

- Processing of personal data related to the breach of a contractual obligation. It is permitted to transfer personal data related to a breach of a contractual obligation to a third party, and the third party is permitted to process this personal data, with the purpose of assessing the creditworthiness of the data subject, or with another similar purpose, and only on condition that the controller or processor has checked the correctness of data, the legal basis for transfer and has registered the data transfer. Gathering data for the aforementioned purposes and transferring it to a third person is not permissible, if the data includes special categories of personal data, the data refers to the fact of being a victim of or committing an offence (before the public hearing, judgement or termination of proceedings), it would have a material adverse effect on the data subjects rights, or less than 30 days or more than 5 years has passed from the end of the breach of the obligation.
- Processing for journalistic purpose – GDPR article 85. It is permissible to process personal data without the data subject's consent for journalistic purposes (primarily make information public in media) if public interest exists and such processing is done according to the principles of journalistic ethics. Such publicising must not cause excessive damage to the rights of a data subject.
- Processing for the purposes of academic, artistic or literary expression – GDPR article 85. It is permissible to process personal data without the data subject's consent for the purposes of academic, artistic or literary expression (primarily publication) if it does not cause excessive damage to the rights of the data subject.
- Processing of personal data in a public space. Unless the law specifies otherwise, in case of the recording of audio or photographic material in a public space, for the purpose of publicizing it, the consent of the data subject shall be replaced with the notification of the data subject in a form which enables him / her to acknowledge the fact of recording and to prevent himself / herself from being recorded. The notification obligation does not exist in case of public events, when the recording of these events for publicizing purposes can be reasonably expected.
- Processing for the purposes of scientific or historical research purposes or for the purposes of official statistics – GDPR article 89. It is permissible to process personal data for these purposes without the data subject's consent in pseudonymized form or in a form that ensures at least equivalent level of data protection.
  De-pseudonymization or other measure of changing non-identifiable personal data to identifiable personal data is only permissible for further research or official statistics. The processor must name the person, who has access to the data that enables de-pseudonymization.
  - The processing of personal data without data subject's consent in a form that the data subject is identifiable is only permissible when:
    - Pseudonymization would make it impossible to achieve the purposes of data processing, or they would be impracticably difficult to achieve;
    - The processor believes that an overwhelming public interest exists;
    - Based upon the processed personal data, the amount of data subject's obligations are not changed and data subject's rights are not excessively damaged in any other way.

- Where the scientific research is based on special categories of personal data, the ethics committee or the DPI will ensure the fulfillment of these obligations.

  Analyses and researches of government institutions, done for the purposes of policy making, is also considered scientific research according to the PDPA.

- The processor or controller is entitled to limit data subjects' rights stated in GDPR articles 15, 16, 18, 21 only to the extent that the enforcement of these rights would probably make the achievement of scientific or historical research purposes, or the purposes of official statistics, impossible or obstruct it considerably.

  - Processing for archiving purposes in the public interest – GDPR article 89. The processor or controller is entitled to limit data subjects' rights stated in GDPR article 15, 16, 18, 19, 20, 21 only to the extent that the enforcement of these rights would probably make the achievement of the purposes of archiving in the

public interest impossible or obstruct it considerably. Limiting data subjects' rights is permissible to protect the records, their authenticity, credibility, integrity and usability.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The PDPA and the Implementation Act do not foresee any derogations / additional requirements to the GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The PDPA and the Implementation Act do not foresee any derogations / additional requirements to the GDPR.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The PDPA and the Implementation Act do not foresee any derogations / additional requirements to the GDPR.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent

for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The PDPA specifies that the DPI is entitled to apply certain special state supervision measures to carry out the necessary state supervision, in addition the DPI is entitled to use the measures specified in article 58 of the GDPR. The DPI may make enquiries to electronic communications undertakings about the data required for the identification of an end-user related to the identification tokens used in the public electronic communications network, except for the data relating to the fact of transmission of messages, unless identification of an end-user is otherwise impossible.

Further, with regard to administrative supervision, the DPI is, if the precepts it issued are not fulfilled, entitled to turn to a

superior agency, person or body of the processor of personal data for organisation of supervisory control or commencement of disciplinary proceedings against an official. Upon failure to comply with a precept of the DPI, DPI may impose a penalty payment pursuant to the procedure provided for in the Substitutive Enforcement and Penalty Payment Act. The upper limit for a penalty payment is 20,000,000 euros or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

In addition to the administrative supervision the DPI may also impose fines (in misdemeanor proceedings) of up to 20,000,000 euros or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The PDPA also specifies the term for review of complaints, *ie,* the DPI shall settle a complaint within 30 days after the date of filing the complaint with the Data Protection Inspectorate. In order to additionally clarify certain circumstances this term may be extended by up to 60 days. If cooperation with other relevant supervisory agencies is required, then the term is extended by a reasonable period necessary to receive the opinion from the other agency.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg,* an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Electronic marketing is regulated by the Electronic Communications Act. As a general rule, the data subject must be able to consent to the electronic marketing. The requirements for this consent depend on whether the addressee is a natural or a legal person, and whether there is an existing client relationship between the parties. Real time non-automated phone calls and regular mail are not considered electronic marketing under Estonian law.

The customer consent must be obtained separately from other terms of the contract between the parties – i.e. it cannot be obtained in the standard terms presented to the customer (*eg,* 'By accepting these terms you agree to receive our commercial communications at the email address provided to us'). In practice, a checkbox separate from the acceptance of the standard terms is often used to obtain this consent.

An opt-in consent is required if the addressee is a natural person, except in the case of an existing client relationship, where opt-out is permissible. The message itself must always include information to clearly determine the person on whose behalf the marketing is sent, clearly distinguishable direct marketing information and clear instructions on how to refuse to receive further direct marketing (*eg,* an unsubscribe link).

Reliance on an opt-out (for natural persons) in the framework of existing client relationships is subject to the following additional requirements:

- the same entity has obtained the contact details in the course of a sale;
- the direct marketing is in respect of similar goods or services;
- the recipient was given a possibility to opt out at the collection of his / her personal data;

- the message must include information to clearly determine the person on whose behalf the marketing is sent; and
- the message must include clearly distinguishable direct marketing information and the recipient is given a simple means in each subsequent email to opt out/unsubscribe.

If the addressee is a legal person, the opt-out system is applicable. There is no need to obtain a prior consent for direct marketing, but:

- the message must include information to clearly determine the person on whose behalf the marketing is sent;
- the message must include clearly distinguishable direct marketing information; and
- the recipient is given a simple means in each subsequent email to opt out / unsubscribe.

ONLINE PRIVACY

Traffic data and location data

Traffic data retention requirements apply only to communications undertakings. Providers of telephone or mobile telephone services and telephone network and mobile telephone network services, as well as providers of Internet access, electronic mail and Internet telephony services are required to preserve for a period of one year network traffic data, location data and associated data thereof which is necessary to identify the subscriber or user in relation to the communications services provided.

Cookies

Due to the opt-out system, consent to cookies is not needed. The law does not refer specifically to browser settings or other applications to be adopted in order to exercise the right to refuse.

The PDPA specifies, that if GDPR article 6(1)(a) is used with regard to providing information society services directly to a child, then the processing of the child's personal data is permitted if the child is at least 13 years old. If the child is younger, then processing is permissible only if and in the extent to which the child's legal representative has agreed to.

KEY CONTACTS

Sorainen
www.sorainen.com/

Kaupo Lepasepp
Partner
T +372 6 400 900
kaupo.lepasepp@sorainen.com

Mihkel Miidla
Partner, Head of Technology & Data Protection
T +372 6 400 959
mihkel.miidla@sorainen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ETHIOPIA

Last modified 23 May 2019

LAW

Ethiopia has several laws that relate to privacy and data security, including the 1995 Constitution of the Federal Democratic Republic of Ethiopia, the 2005 Criminal Code of the Federal Democratic Republic of Ethiopia, the 1960 Civil Code, the Computer Crime Proclamation No. 958/2016 and the Freedom of the Mass Media and Access to Information Proclamation No. 590/2008.

DEFINITIONS

Definition of Personal Data

No specific definition is generally applicable.

The Freedom of the Mass Media and Access to Information Proclamation No. 590/2008, applicable to government entities, is understood to generally define personal data as information about an identifiable individual that relates, but is not limited, to:

- medical, education, academic, employment, financial transaction, professional or criminal history
- ethnic, national or social origin, age, pregnancy, marital status, color, sexual orientation, physical or mental health, well-being, disability, religion, belief, conscience, culture, language or birth
- an identification number, symbol or other identifier assigned to the individual, address, fingerprints or blood type
- personal opinions, views or preferences, except as relate to another individual
- views or opinions on grant proposals, awards, or prizes granted to another individual, provided such views or opinions are not associated with the other individual's name
- views or opinions of others about the individual, or
- an individual's name, in combination with other personal data, or alone, if could reasonably be linked to personal data (exception applies for persons deceased for more than 20 years).

Definition of Sensitive Personal Data

Sensitive personal data is not defined.

NATIONAL DATA PROTECTION AUTHORITY

There is no data protection authority.

REGISTRATION

There is no requirement to register databases or personal data processing activities.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

Though Ethiopia has not enacted a specific law to address personal data collection and processing issues, the country's scattered legislative framework is understood to require that personal data be collected and processed with due care and only for an intended lawful purpose.

TRANSFER

No specific geographic transfer restrictions apply in Ethiopia.

However, existing law provides that personal data transfers must be based on the prior written consent of the person whose data is to be transferred and only for an intended lawful purpose.

SECURITY

There are no specific data security requirements.

The Computer Crime Proclamation No. 958/2016 requires service providers to implement reasonable and necessary security measures to protect confidential computer traffic data disseminated through their computer systems or communications services from unlawful and unnecessary access.

BREACH NOTIFICATION

There is no general breach notification requirement in Ethiopia.

However, the Computer Crime Proclamation No. 958/2016 requires service providers with knowledge that a crime stipulated by the Proclamation (including breach of privacy via unauthorized access) has been committed by a third party through the computer system it administers to immediately notify the Information Network Security Agency, report the crime to police, and take appropriate measures.

ENFORCEMENT

Ethiopian courts are responsible for enforcing data protection and privacy provisions in the law.

ELECTRONIC MARKETING

No specific law regulates electronic marketing in Ethiopia.

ONLINE PRIVACY

There are several provisions in Ethiopian law to regulate online privacy. For example, the Computer Crime Proclamation No. 958/2016 criminalizes the unauthorized access to, and illegal interception and damage of, computer data.

The Proclamation further prohibits the use of computer systems to disseminate advertisements absent addressee consent.

KEY CONTACTS

Benyam Tafesse
Head, Employment, IP & Aviation Practices
Mehrteab Leul & Associates
T +251 115 159 798
benyam@mehrteableul.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

FINLAND

Last modified 10 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

Finland has passed a supplementary implementation act of the GDPR, the Data Protection Act of Finland (*Tietosuojalaki*), which enters into force on January 1, 2018.

Other key Finnish laws concerning data privacy and protection are: the Act on Electronic Communication Services 917/2014 (*Laki sähköisen viestinnän palveluista*) of January 1, 2015, which aims to, inter alia, ensure the confidentiality of electronic communication and the protection of privacy; the Act on the Protection of Privacy in Working Life 759/2004 ('Working Life Act') (*Laki yksityisyyden suojasta työelämässä*), which aims to promote the protection of privacy and other rights safeguarding the privacy in working life, and; the Act on the Processing of Personal Data in Criminal Cases and in connection with Maintaining National Security, which enters into force on January 1, 2019 along with the Data Protection Act.

The Working Life Act includes some specific provisions on privacy issues relating to employment and work environments such as right to monitor employees' email communication. The protection of employees' privacy has traditionally been strict in Finland and Finland will use the national leeway provided in the GDPR with regard to processing of personal data in the context of employment and maintain the specific law concerning privacy in working life. Some minor amendments

will be made to the Working Life Act and a Government Proposal regarding these amendments has been given in July 2018. The amendments have not yet been passed, but the objective is that the amended act shall enter into force as soon as possible.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions in Finland are the same as in the GDPR and no additional local definitions have been included.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

In Finland The Office of the Data Protection Ombudsman (*Tietosuojavaltuutetun toimisto*) is the local supervisory authority. The Office of the Data Protection Ombudsman contains the Data Protection Ombudsman himself, two Assistant Data

Protection Ombudsmen as well as various data protection experts and secretaries as public servants.

Post address: Visiting address: P.O. Box 800 Ratapihantie 9, 6th floor 00521 Helsinki Finland

T +358 29 56 66700

tietosuoja@om.fi www.tietosuoja.fi

The Data Protection Act specifies the Data Protection Ombudsman's duties and rights under the GDPR regarding *eg*, audits, right to receive information and right to impose sanctions on entities.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

The Finnish Data Protection Act does not contain any provisions related to registration. The former Finnish Personal Data Act did contain some requirements for registration, but these have been repealed.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

In Finland the new Data Protection Act does not contain specific local requirements on data protection officers. However, few special national acts stipulate mandatory appointment of data protection officers.

For example, in Finland all functional units of healthcare and social welfare as well as pharmacies must appoint a data protection officer under the Act on Electronic Prescriptions 2007/61 (*Laki sähköisestä lääkemääräyksestä*). This requirement is also set in the Act on Electronic Processing of Client Information in Social Welfare and Healthcare 2007/159 (*Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä*) (the 'Act on Electronic Processing of Client Information') to all functional units of the public social welfare and healthcare section as well as the Finnish Social Insurance Institution ('KELA'). However, a Government Proposal has been given on amending certain sections of the Act on Electronic Processing of Client Information. Due to the proposed amendment, the section covering the appointment of a data protection officer will be amended and the requirement removed due to obligation for public entities to appoint a data protection officer already being included in the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose

- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Finland has used the national leeway provided in GDPR article 6(1) subsection e) as well as GDPR article 9(2) subsections b), g), h), i) and j) regarding collecting and processing personal data in certain situations.

In Finland, personal data may be processed under GDPR article 6(1) e) when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, if:

it relates to information representing a person's position, tasks and the processing thereof in the public sector entity, business life or other equivalent activity, the purpose of processing rests on the public interest grounds and it complies with the principle of proportionality;

- it is necessary in the operation of authorities in order to perform a task in public interest and it complies with the principle of proportionality;
- it is necessary for scientific or historical research or statistical purposes and it complies with the principle of proportionality; or
- the processing of research material, material related to cultural heritage and any description information thereof for archiving purposes is necessary on public interest grounds and complies with the principle of proportionality.

The processing of special categories of personal data under GDPR article 9(2) subsections b), g), h), i) and j) may be carried out in Finland if it concerns, by way of example:

- personal data of the insured person or a claimant within the operation of an insurance company to settle its liability;
- health and medical data in connection with certain operations of healthcare and social welfare service providers; or
- processing for scientific or historical research purposes or statistical purposes.

In addition to the above-mentioned processing activities, the national leeway has also been used in the Data Protection Act with respect to processing related to criminal convictions and offences as well as processing of national identification numbers. For example in relation to national identification numbers, processing is only allowed based on data subject consent or if it is necessary to unambiguously identify the data subject for: a) a task defined in law, b) realization of the rights and responsibilities of the data subject or data controller, or c) historical or scientific research or statistical purposes. Further, national identification numbers can be processed for e.g. credit, loan, insurance, debt collection, payment service and leasing purposes, in social or healthcare services, and in connection with employment relatioships.

The Working Life Act sets additional processing requirements to employment related data that an employer collects and processes of its employees. All employee personal data processed must at all times be directly necessary for the employee's employment relationship. This necessity requirement cannot be bypassed even with the employee's consent.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or

g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The new Data Protection Act does not include additional clauses concerning transfer of personal data, *ie,* Finland has decided not to use the marginal national leeway provided in GDPR articles 46 and 49 as per now.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The new Finnish Data Protection Act does not contain any direct additional requirements for the security of processing in the meaning of GDPR article 32. However, the Data Protection Act does specify the security measures to be taken if special categories of personal data are processed. These measures are mostly the same as included in the GDPR article 32 (*eg,* pseudonymization, encryption, personnel training, access management, log-on data usage), and according to the government proposal explanatory text serve more as examples of what measures must be taken rather than an exhaustive mandatory list despite the wording used.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

In Finland the general breach notification procedure follows the rules set by GDPR.

However, certain special national legislation does include additional requirements on breach notifications. The Act on Electronic Communication Services establishes an obligation for telecommunications operators to notify their subscribers, users and the Finnish Transport and Communications Authority ('Traficom') of significant information security violations or threats and of anything else that prevents or significantly interferes with communication services. In addition, under the Act on Electronic Communication Services, domain name registrars shall notify Traficom without undue delay of significant violations of information security in its domain name services and of anything that essentially prevents or disturbs such services.

The Act on Strong Electronic Identification and Electronic Signatures (2009/617) (*Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista*) also states that an electronic identification service provider shall notify service providers using its services, identification device holders as well as Traficom of severe risks and threats to its data security.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

In Finland The Data Protection Ombudsman and the Assistant Data Protection Ombudsmen supervise compliance with GDPR and the Finnish Data Protection Act. In addition, an Expert Committee provides statements on significant questions and matters related to data processing upon the request of the Data Protection Ombudsman.

The Data Protection Ombudsman may order a data controller or data processor to comply with certain articles of the GDPR as well as Section 18 of the Data Protection Act, which covers the Data Protection Ombudsman's right to receive necessary information, and impose a default fine to make the order more effective. However, the default fine may not be imposed on a natural person due to them not complying with the section on the Data Protection Ombudsman's right to receive information if the person is suspected of a crime and the information is related to the alleged crime.

Administrative fines defined in article 83 of the GDPR will be issued by a sanction board within the Office of the Data Protection Ombudsman. The sanction board consists of the Data Protection Ombudsman and the two Assistant Data Protection Ombudsmen and the decision shall be made as a majority decision. Finland has decided to use the provided national leeway and the Act regulates that the administrative fines cannot be issued to:

- state authorities;
- state-owned businesses;
- local authorities;
- independent public institutions;
- organs operating in connection with the Parliament;
- the Office of the President of the Republic; or
- the Evangelical Lutheran Church of Finland or the Orthodox Church of Finland or the parishes, associations of parishes or other bodies thereof.

In addition, criminal sanctions can ensue from breaches of data protection laws in Finland as the Criminal Code of Finland 39/1889 (*Rikoslaki*) includes several data processing, data privacy, confidentiality and data security related offences or crimes. Finland has also introduced a new punishable offence, the data protection offence, to the Criminal Code of Finland based on the GDPR. If the controller or data processor commits a data protection offence, the punishment is a fine or up to one year of imprisonment. The Criminal Code also states that the prosecutor is obligated to hear the Data Protection Ombudsman before bringing charges against a controller or data processor for a data protection offence.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Act on Electronic Communication Services regulates direct marketing by electronic means in Finland. The Data Protection Ombudsman is the supervising authority also in compliance issues with the Act on Electronic Communications Services' provisions concerning direct marketing.

Direct marketing to natural persons is only allowed by means of automated calling systems, facsimile machines, or email, text, voice, sound or image messages and only if the natural person has given his / her prior consent to it. Direct marketing using other means is allowed if the natural person has not specifically forbidden it. If, however, a service provider receives an email address, number or other contact information in relation to the sale of product or service, the service provider may normally use this contact information to directly market the service providers own products or services belonging to the same product group or that are otherwise similar to the natural person in question. The natural person must be able to easily and at no charge unsubscribe from or prohibit any direct marketing and the service provider must clearly inform the natural person of that possibility.

A service provider may use direct marketing with legal persons (businesses) unless they have specifically prohibited it. As

with natural persons, legal persons must also be able to easily and at no charge unsubscribe from/prohibit any direct marketing and the service provider must clearly inform the legal person of that possibility. In addition, telecommunications operators and corporate or association subscribers are entitled, at a user's request, to prevent the reception of direct marketing.

The Data Protection Ombudsman and the Finnish Customer Marketing Association have given their interpretations on B2B direct marketing using a legal person's general contact information, such as an email address (e.g. info@company.com). If the B2B direct marketing is sent to a legal person's employee's personal work email (fistname.lastname@company.com), the person's prior consent is required unless the marketed product or service is substantially related to the person's work duties based on the person's job description.

Email, text, voice, sound or image message sent for the purpose of direct marketing must be clearly and unmistakably be recognized as direct marketing. It is forbidden to send such a direct marketing message that:

- disguises or conceals the identity of the sender on whose behalf the communication is made;
- is without a valid address to which the recipient may send a request that such communications be ended;
- solicits recipients to visit websites that contravene with the provisions of the Consumer Protection Act 20.1.1978/38 (*Kuluttajansuojalaki*).

If any processing of personal data is involved in the electronic direct marketing, the provisions of the applicable data protection laws (such as the Finnish Data Protection Act and the GDPR) will also apply.

ONLINE PRIVACY

The Information Society Code regulates online privacy matters such as the use of cookies and location data.

Cookies

A service provider is allowed to save cookies and other data in a user's terminal device, as well as use such data, only with the consent of the user. The consent can be given via web browser or other applicable settings. The service provider must also give the user clear and complete information on the purposes of use of cookies.

However, the above restrictions do not apply to use of cookies only for the purpose of enabling the transmission of messages in communications networks or which is necessary for the service provider to provide a service that the subscriber or user has specifically requested.

Location Data

The location data associated with a natural person can be processed for the purpose of offering and using added value services, if:

- The user or subscriber, whose data is in question, has given his/her consent
- If the consent is otherwise clear from the context, or
- Is otherwise provided by law.

In general, location data may only be processed to the extent necessary for the purpose of processing and it may not limit the privacy any more than absolutely necessary.

The value added service provided shall ensure that:

- The user or subscriber located has easy and constant access to specific and accurate information on his / her location data processed, purpose and duration of its use and if the location data will be disclosed to a third party for the purpose of providing the services

- The above mentioned information is available and accessible to the user or subscriber prior him/her giving his/her consent
- The user or subscriber has the possibility to easily and at no separate charge cancel the consent and ban the processing of his / her location data (if technically feasible).

The user or subscriber is entitled to receive the location data and other traffic data showing the location of his / her terminal device from the value added service provider or the communications provider at any time.

The Act on Electronic Communication Services regulates online privacy matters such as the use of cookies and location data.

Cookies

A service provider is allowed to save cookies and other data in a user's terminal device, as well as use such data, only with the consent of the user. The service provider must also give the user clear and complete information on the purposes of use of cookies.

The Finnish authorities have stated that cookie consent can be given via web browser or other applicable settings, and that the information does not need to be given using a separate pop-up window. This was nonetheless stated prior to the GDPR and its consent / transparency requirements, and is not necessarily in line with the GDPR requirements. The local authorities have not issued updated guidelines on the matter as of now.

However, the above restrictions do not apply to use of cookies only for the purpose of enabling the transmission of messages in communications networks or which is necessary for the service provider to provide a service that the subscriber or user has specifically requested.

Location Data

The location data associated with a natural person can be processed for the purpose of offering and using added value services, if;

- the user or subscriber, whose data is in question, has given his / her consent;
- if the consent is otherwise clear from the context; or
- is otherwise provided by law.

In general, location data may only be processed to the extent necessary for the purpose of processing and it may not limit the privacy any more than absolutely necessary. The value added service provided shall ensure that:

- the user or subscriber located has easy and constant access to specific and accurate information on his / her location data processed, purpose and duration of its use and if the location data will be disclosed to a third party for the purpose of providing the services:
- the above mentioned information is available and accessible to the user or subscriber prior him / her giving his/her consent;
- the user or subscriber has the possibility to easily and at no separate charge cancel the consent and ban the processing of his / her location data (if technically feasible).

The user or subscriber is entitled to receive the location data and other traffic data showing the location of his/her terminal device from the value added service provider or the communications provider at any time.

KEY CONTACTS

Markus Oksanen
Partner
T +358 9 4176 0431
markus.oksanen@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

FRANCE

Last modified 23 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

France adapted its domestic legislation to GDPR with the enactment of (i) Law No. 2018-493 of June 20, 2018 on the protection of personal data, which mainly updates Law No. 78-17 of January 6, 1978 on information technology, data files and civil liberties, the principal law regulating data protection in France (the "**Law**") and (ii) Decree No. 2018-687 of 1 August 2018 implementing the Law, which updates the Decree No. 2005-1309 of 20 October 2005 (the "**Decree**").

In addition, the Order No. 2018-1125 of December 12, 2018, adopted pursuant to Article 32 of Law No. 2018-493, updates the Law and other French laws relating to personal data protection in order to "*simplify the implementation and make the necessary formal corrections to ensure consistency with EU data protection law*" (the "**Order**"). The Order will enter into force on June 1, 2019. The Decree will be amended before June 1, 2019 by another decree, in order to take into account the revisions introduced by the Order.

Territorial Scope

As of today, the Law provides that it applies when the data controller is either (i) established in France or (ii) established outside the European Union and uses processing means located on the French territory.

As revised by the Order and as from June 1, 2019, the territorial scope of the Law will be aligned with Article 3 of GDPR.

In this respect, the Law will apply to any processing of personal data in the context of the activities of an establishment of a controller or a processor in France, regardless of whether the processing takes place in France or not. In addition, French rules adopted on the basis of the leeway left to Member States by the GDPR will apply only to the extent the **data subject resides** in France, including when the data controller is not established in France, with an exception for processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression. For such processing activities, the national rules of the Member State where the data controller is established apply, to the extent such controller is established in the European Union.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions under the Law are the same as under the GDPR. The Order creates an express reference to GDPR definitions within the Law, thus harmonizing the definitions and concepts of French law with the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The « Commission Nationale de l'Informatique et des Libertés » or « CNIL » is the French Supervisory Authority

3 place de Fontenoy

TSA 80175

75334 Paris Cedex 07

1. 01 53 73 22 22
2. 01 53 73 22 00

https://www.cnil.fr/en/home

The CNIL has different missions and powers, which mainly include (i) informing data subjects and data controllers/processors (whether public or private) about their rights and obligations; (ii) ensuring compliance of all personal data processing with French and EU data protection rules as well as data protection rules resulting from international commitments of France; (iii) anticipating new challenges and issues arising from innovation and the use of new technologies, including privacy in general and ethics; (iv) controlling and sanctioning. In addition, the Law provides for mutual assistance and joint operations with other EU Supervisory Authorities, as well as cooperation with non-EU supervisory authorities.

The CNIL has a range of tools to complete its missions, including *eg,* publication of guidelines, recommendations and standards, approval of codes of conduct, certifications and labels, broad range of on-site and off-site investigation powers and sanctions. The Order provides further precisions on the functioning of the CNIL and its specific tasks and powers, notably the extent of on-site investigations and procedural requirements, in connection with the missions described above.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Prior formalities with the CNIL are no more required and are replaced by the obligation to hold a record of processing which include the same categories of information as those initially requested in the filing forms.

However, formalities are maintained for the processing of health data which is subject either to a declaration of conformity to specific requirements defined by the CNIL or an authorization by the CNIL. In this respect, the CNIL has published several methodologies of reference ("*Méthodologies de Référence*" or "MR") in July 2018 and is in the process of drafting additional matters-specific reference methodologies (*e.g.* research, studies and evaluations that do not involve human person). A formal commitment to comply with these methodologies exempts the data controller – generally the sponsor of the research – from having to apply for a formal authorization with the CNIL.

Certain specific processing of personal data must be authorized by decree of the State Council (*Conseil d'Etat*) or ministerial order, taken after a motivated and public opinion of the CNIL. These processing are as follows:

- Processing of the social security number (with a few exceptions);
- Processing carried out by or on behalf of the State, acting in the exercise of its public authority prerogatives, of genetic or biometric data necessary to the authentication or identity control of individuals;
- Processing carried out on behalf of the State (i) which concern State security, defense, national security, or (ii) which purpose is the prevention, investigation, detection or prosecution of criminal offences, or enforcement of criminal convictions or security measures.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Law provides that controllers processing personal data under the scope of the EU Data Protection Directive on Police and Criminal Justice Cooperation must appoint a DPO, with the exception of jurisdictions acting within the scope of their judicial activity.

The Decree specifies the mandatory information to be communicated to the CNIL by data controller(s) or processor(s) in the DPO notification form.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to

processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Special Category Data

The Law contains specific provisions regarding the processing of health data, as well as additional provisions regarding processing of sensitive personal data.

As from June 1, 2019, the Order will suppress the exemption that previously applied to processing of special categories of data where such data would be promptly subject to an anonymization process.

Criminal Convictions and Offences data

The following categories of persons can process such personal data:

- Courts, public authorities and legal persons entrusted with a public service, acting within the scope of their legal functions, as well as entities collaborating with judicial entities as listed in the Decree;
- Auxiliaries of justice, for the strict exercise of their functions;
- Individuals and private entities to prepare, bring or defend a claim in court as a victim or defendant, and to execute the court decision, for the duration strictly necessary for these purposes. It is possible to share such information with third parties under the same conditions and for the same purposes;
- Collective IP rights management organizations for the purpose of defending those rights; and
- Persons reusing public information appearing in published rulings, provided that the processing has neither the purpose or effect of allowing the re-identification of the concerned persons.

In addition, the following categories of persons are authorized by the Decree to process personal data relating to criminal convictions, offenses or related security measures:

- Victims support associations contracted by the Ministry of Justice;
- Associations of assistance to the reintegration of persons placed under the authority of justice, in the respect of their social object;
- The establishments and services mentioned in 2 ° of I of Article L. 312-1 of the Code of Social Action and Families as part of their mission of medico-social support;

- The establishments and services mentioned in 4 ° and 14 ° of I of Article L. 312-1 of the Code of Social Action and Families;
- The drop-in and reception centers mentioned in III of Article L. 312-1 of the Code of Social Action and Families;
- The medical or medico-educational establishments authorized mentioned in articles 15 and 16 of the order No. 45-174 of February 2, 1945 relating to delinquent childhood;
- The public or private educational or vocational training institutions, authorized and appropriate boarding schools for juvenile school-aged offenders mentioned in Articles 15 and 16 of the aforementioned order of February 2, 1945;
- Private legal entities exercising a public service mission or the authorized associations mentioned in Article 16 of the aforementioned order of February 2, 1945;
- The legal representatives for the protection of the adults mentioned in Article L. 471-1 of the Code of Social Action and Families.

The CNIL may issue standard regulations, prescribe additional measures to be implemented, including of a technical and organizational nature, and / or complementary warranties for processing of special categories of data, including notably criminal convictions and offences data, by public and private entities (except for processing carried out in connection with the exercise of public authority by or on behalf of the State).

In addition, processing of criminal convictions and offences data which purpose is the prevention, investigation, detection or prosecution of criminal offences, or enforcement of criminal convictions or security measures by or on behalf of the State is subject to an order of the competent Ministry.

Transparency (Privacy Notices)

The Law mandates data controllers to provide data subjects with information relating to their right to define directives relating to the processing of their personal data after their death (digital legacy).

In addition, where the data is collected from a data subject under 15, the data controller must provide the mandatory information provided for by Art. 13 GDPR in a clear and easily accessible language.

Rights of the Data Subjects

The Decree describes the conditions in which the data subjects can exercise their rights.

Data subjects' rights can be restricted notably to avoid obstructing administrative investigations, inquiries or procedures, to safeguard the prevention, investigation, detection and prosecution of criminal offences, as well as of administrative enquiries, or to protect the rights and freedoms of others.

Digital legacy

Data subjects have the right to give instructions regarding the storage, deletion and communication of their personal data after their death. Such instructions can be either:

- General, in which case they apply to all their personal data, irrespective of who the controller is. Such instructions can be given to a trusted third party certified by the CNIL; however, the implementing decree in this respect has never been adopted since the adoption of this provision in 2016; or
- Special, in which case the data subject can also give his / her instructions to the relevant data controller. It is required to obtain the specific consent of the data subject, and such consent cannot derive from his/her consent to general terms and conditions.

If the data subject has not given any instructions in his / her lifetime, then his / her heirs can exercise certain rights, in particular:

- The right of access, if it is necessary for the settlement of the succession; and
- The right to object to close the deceased's accounts and cease the processing of his / her personal data.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

In the event processing of personal data involves a transfer of data outside the European Union territory, data subjects must be provided with mandatory information on, inter alia, the data transferred, the purpose of the transfer, the recipients of the data and the transfer mechanism used in accordance with the GDPR.

With respect to transfers made on the basis of Article 49(1)§2 of GDPR ("compelling legitimate interest"), the Decree provides that the CNIL will define templates (including annexes) to be used by data controllers to inform the CNIL about such transfers.

With respect to transfers made on the basis of code of conduct or other certification mechanism approved by the CNIL in accordance with the Law and the Decree, the Decree provides that data controller / data processor that rely on such transfer mechanisms shall provide the CNIL with a binding and enforceable commitment to apply appropriate safeguards to data subjects' rights and freedoms in the concerned third-country.

In addition, where a data subject seizes the CNIL about the validity of a data processing involving a transfer of personal data outside the European Union, the CNIL may require the State Council (Conseil d'Etat) to order the suspension of a such transfer and require the State Council to send a reference for a preliminary ruling to the European Court of Justice

aiming at evaluating the validity of any adequacy decision or other legislative act adopted by the European Commission pursuant to Articles 45 and 46 of GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

No specific requirements other than those set forth in the GDPR.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Decree restricts the obligation of notification under Article 34 of the GDPR for the following processing:

Processing including personal data allowing to identify, directly or indirectly, individuals whose identity is protected under

Article 39 sexies of the French law on the freedom of the press; and

- Administrative, financial and operational data, as well as health data processing for which the notification of an unauthorized disclosure or access is likely to result in a risk for the national security, defense or public, due to the volume of data affected by the breach and the private information it contains (such as the family address or composition).

The Order provides that a Decree by the State Council, adopted after seeking the CNIL's opinion (likely to be adopted before June 1, 2019), will specify a list of categories of processing and processing operations that derogate to the data breach notification requirement. Such derogation will only apply to processing that are necessary pursuant to a legal obligation bearing on the data controller or a public interest mission vested in the data controller, where such data breach notification would likely result in a risk to homeland security, defense or public safety.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg,* an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Law does not contain explicit provisions with respect to electronic marketing. However, Article L. 34-5 of the French Postal and Electronic Communications Code regulates electronic marketing in France. The CNIL has issued guidelines on the basis of this provision.

The CNIL distinguishes between B2B and B2C relationships.

In any event, all electronic marketing messages must specify the name of the advertiser and allow the recipient to object to the receipt of similar messages in the future.

Electronic marketing to consumers (B2C)

Electronic marketing activities are authorised provided that the recipient has given consent at the time of collection of his / her email address.

This principle does not apply when:

- the concerned individual is already a customer of the company and if the marketing messages sent pertain to products or services similar to those already provided by the company, or
- the marketing messages are not commercial in nature.

In any event the concerned individual, at the time of collection of his / her email address, must:

- be informed that it will be used for electronic marketing activities, and
- be able to easily and freely object to such use.

Electronic marketing to professionals (B2B)

Electronic marketing activities are authorized provided that the recipient has been, at the time of collection of his / her email address:

- informed that it will be used for electronic marketing activities, and
- able to easily and freely object to such use.

The message sent must relate to the concerned individual's professional activity.

Please note that email addresses such as *contact@companyname.fr* are not subject to the requirements of prior consent and the right to object.

ONLINE PRIVACY

Cookies

The EU Cookie Directive has been implemented in the Law. It states that any subscriber or user of electronic communications services must be fully and clearly informed by the data controller or its representative of:

- the purpose of any cookie (*ie,* any means of accessing or storing information on the subscriber's / user's device, *eg,* when visiting a website, reading an email, installing or using software or an app), and
- the means of refusing cookies,

unless the subscriber / user has already been so informed.

Cookies are lawfully deployed only if the subscriber / user has expressly consented after having received such information. Valid consent can be expressed via browser settings if the user can choose the cookies he / she accepts and for which purpose.

However, the foregoing provisions do not apply:

- to cookies the sole purpose of which is to allow or facilitate electronic communication by a user, or
- if the cookie is strictly necessary to provide online communication services specifically requested by the user.

In December 2013 the CNIL issued updated recommendations for cookies that are more flexible than the CNIL's prior position. The CNIL considers that certain cookies are not covered by the Law (*eg,* cookies used to constitute a 'basket' on a e-commerce platform, session ID cookies authentication cookies and certain analytics cookies).

Regarding consent, the CNIL has specified that consent must be:

- freely given (*ie,* in circumstances where the user has a choice to refuse consent)
- specific (*ie,* relate to a specific cookie associated with a clearly defined purpose), and

- informed (*ie,* the user must be given information beforehand, specifying the cookie's purpose as well as the possibility to revoke consent).

The CNIL regards the following consent collection mechanisms as compliant:

- a banner on the first webpage visited (of a particular site), which can specify *eg,* that continuing to visit the site constitutes consent to set cookies
- a consent request zone overprinting on the site's homepage
- boxes to tick when registering for an online service, and
- buttons that activate functionalities of services that set cookies (such as plug-ins on social networks).

The CNIL considers that the obligation of obtaining the user's prior consent is incumbent on website publishers, mobile application publishers, advertisers ("*régies publicitaires*"), social networks, analytics services providers, etc., which must all comply with the Law, whether they deploy or read cookies on their own or a third party website or application.

Location and Traffic Data

The Postal and Electronic Communications Code deals with the collection and processing of location and traffic data by electronic communication service providers (CSPs).

All traffic data held by a CSP must be erased or anonymised. However, traffic data may be retained, for example:

- for the purpose of finding, observing and prosecuting criminal offences
- for the purpose of billing and payment of electronic communications services, or
- for the CSP's marketing of its own communication services, provided the user has given consent thereto.

Subject to exceptions (observing and prosecuting criminal offences; billing and payment of electronic communications services), location data may be used in very limited circumstances, for example:

- during the communication, for the proper routing of such communication, and
- where the subscriber has given informed consent, in which case the location data may be processed and stored after the communication has ended. Consent can be revoked free of charge at any time.

KEY CONTACTS

Denise Lebeau-Marianna
Partner, Head of Data Protection Practice - EuroPriSe Expert
T + 33 (0)1 40 15 24 98
denise.lebeau-marianna@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

GERMANY

Last modified 17 October 2018

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

Germany has adjusted the German legal framework to the GDPR by passing the new German Federal Data Protection Act (*Bundesdatenschutzgesetz* – 'BDSG'). The BDSG was officially published on July 5, 2017 and came into force together with the GDPR on May 25, 2018. The purpose of the BDSG is especially to make use of the numerous opening clauses under the GDPR which enable Member States to specify or even restrict the data processing requirements under the GDPR.

Find the English version here.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions are the same as in Art. 4 GDPR. Beyond that, the BDSG (New) contains further definitions for 'public bodies of the Federation', 'public bodies of the *Länder*' and 'private bodies' in Sec. 2 BDSG (New).

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Germany does not have one central Data Protection Authority but a number of different Authorities for each of the 16 German states (*Länder*) that are responsible for making sure that data protection laws and regulations are complied with. In addition the German Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte für Datenschutz und Informationsfreiheit* – 'BfDI') is the Data Protection Authority for telecommunication service providers and represents Germany in the European Data Protection Board. To ensure that all the Authorities have the same approach a committee consisting of members of all Authorities has been established – the 'Data Protection Conference' (*Datenschutzkonferenz* 'DSK'). The coordination mechanism between the German Authorities mirrors the consistency mechanism under the GDPR.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general

notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

There are no registration requirements in Germany.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The threshold to designate a Data Protection Officer (DPO) is much lower in the BDSG. The controller and processor has to designate a DPO if they constantly employ as a rule at least ten persons dealing with the automated processing of personal data, Sec. 38 (1) first sentence BDSG. The meaning of 'automated processing' is interpreted broadly by the German Authorities. It basically covers every employee who works with a computer.

If the threshold of 10 persons is not reached, Sec. 38 (1) second sentence BDSG regulates in addition to Art. 37 GDPR, that a DPO has to be designated in case the controller or processor undertakes processing subject to a data protection impact assessment pursuant to Art. 35 GDPR, or if they commercially process personal data for the purpose of transfer, of anonymized transfer or for purposes of market or opinion research.

Furthermore, a dismissal protection for the DPO is provided in Sec. 38 (2) in conjunction with Sec. 6 (4) BDSG. The dismissal of the data protection officer is only permitted in case there are facts which give the public body just cause to terminate without notice. After the activity as data protection officer has ended, the data protection officer may not be terminated for a year following the end of appointment, unless the public body has just cause to terminate without notice.

Additionally, Sec. 38 (2) in conjunction with Sec. 6 (5) and (6) BDSG stipulates that the data protection officer shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless they are released from this obligation by the data subject. Moreover, the right to refuse to give evidence of a head of a public body or a person employed by such a body also applies for the DPO.

Moreover, the German Authorities require that the DPO speaks the language of the competent Authorities and data subjects, ie German, or at least that instant translation is ensured.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);

- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the

data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The BDSG has additional rules regarding processing of special categories of personal data. Contrary to Art. 9 (1) GDPR, processing of such data is permitted by public and private bodies in some cases, see Sec. 22 (1), 23 (3) BDSG. Also, Sec. 23 BDSG (New) determines cases in which controllers are permitted to process data for a purpose other than the one for which the data were collected.

Section 4 BDSG (New) provides a special rule for video surveillance of publicly accessible areas, which is not applicable. According to the German DPAs as well as the unanimous opinion in German legal literature the provision is generally not compliant with the GDPR and therefore must not be applied due to the general principle of the primacy of Union law. This is based in the argument that the GDPR does not contain any opening clause for deviating from Art. 6 para. 1 lit. f) GDPR with respect to video surveillance.

Furthermore BDSG provides special rules regarding processing for employment-related purposes in Sec. 26 BDSG. The German legislator has made very broad use of the opening clause in Art. 88 (1) GDPR and has basically established an own employee data protection regime. This new rules reflect the current German employee privacy rules which also has the consequence that a set of case law of the German Federal Labour Court (*Bundesarbeitsgericht* – 'BAG') will apply. In case the processing is conducted for employment-related purposes it is subject to Sec. 26 BDSG only and a recourse to the general legal grounds set out in Article 6 GDPR are blocked. Personal data of employees can only be processed in the

employment context (setting aside some very special cases under the BDSG when it comes to the assessment of the working capacity of the employee and other handling of special categories data as well as exchange of data with the works council) in these cases:

- The processing is necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract (Sec. 26 (1) sentence 1 BDSG) (please note that the BAG interprets the predecessor provision broader than Art. 6 (1) (b) GDPR)
- Employees' personal data may be processed to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the processing of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason (Sec. 26 (1) sentence 2 BDSG)
- The processing is based on a works council agreement which complies with the requirements set out Art. 88 para. 2 GDPR (Sec. 26 (4) BDSG)
- The processing is based on the written employee consent. A derogation from the written form can apply if a different form is appropriate because of special circumstances. This derogation will most likely never apply in practice. Moreover, the utilization of consent as basis for the processing is particularly problematic in Germany as Sec. 26 (2) BDSG stipulates requirements in addition to Art. 7 GDPR. If personal data of employees are processed on the basis of consent, then the employee's level of dependence in the employment relationship and the circumstances under which consent was given shall be taken into account in assessing whether such consent was freely given. Consent may be freely given in particular if it is associated with a legal or economic advantage for the employee, or if the employer and employee are pursuing the same interests. The German DPAs interpret this provision in a way that employee consent cannot be used for processing of personal data which directly relates to the employment relationship, but only to supplementary services offered by the employer (*eg*, private use of company cars or IT equipment, health management or birthday lists).

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or

g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The same applies as in Article 44 et seqq. GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The BDSG has additional rules regarding the processing of special categories of personal data in Sec. 22 (2) BDSG. In case of processing of such data, appropriate and specific measures have to be taken to safeguard the interests of the data subject.

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following:

- technical organizational measures to ensure that processing complies with Regulation (EU) 2016/679
- measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed
- measures to increase awareness of staff involved in processing operations
- designation of a data protection officer
- restrictions on access to personal data within the controller and by processors
- the pseudonymization of personal data
- the encryption of personal data
- measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and

services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing
- specific rules of procedure to ensure compliance with this Act and with the GDPR in the event of transfer or processing for other purposes

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The regulations regarding the breach of notification are mainly identical to Art. 33, 34 GDPR.

Sec. 29 (1) BDSG stipulates in addition to the exception in Art. 34 (3) GDPR, the obligation to inform the data subject of a personal data breach according to Art. 34 GDPR shall not apply as far as meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. By derogation from previous, the data subject pursuant to Article 34 GDPR shall be informed if the interests of the data subject outweigh the interest in secrecy, in particular taking into account the threat of damage.

According to Sec, 43 (3) BDSG, a notification pursuant to Art. 33 GDPR or a communication pursuant to Article 34 (1) GDPR may be used in proceedings pursuant to the Act on Regulatory Offences (*Gesetz über Ordnungswidrigkeiten* – 'OWiG') against the person required to provide a notification or a communication only with the consent of the person obligated to provide a notification or a communication.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that

'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Regarding the enforcement the German Authorities declared that they are of the opinion that the fines will not only be calculated based on the turnover of the specific affected company, but of the entire group of undertakings. However, whether this interpretation of Art. 83 (4), (5) and (6) GDPR in connection with Recital 150 GDPR is correct is currently highly disputed in Germany with solid arguments against this broad interpretation. The enforcement of fines is subject to the Act on Regulatory Offences (*Gesetz über Ordnungswidrigkeiten* – 'OWiG'), other sanctions, *eg,* a temporary or definitive limitation or ban on processing, is subject to the rules regarding administrative procedures.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg,* an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

In general, unsolicited electronic marketing requires prior opt-in consent. The opt-in requirement is waived under the 'same service/product' exemption. The exemption concerns marketing emails related to the same products/services as previously purchased from the sender by the user provided that:

- the user has been informed of the right to opt-out prior to the first marketing email
- the user did not opt-out, and
- the user is informed of the right to opt-out of any marketing email received. The exemption applies to electronic communication such as electronic text messages and email but does not apply with respect to communications sent by fax.

Direct marketing emails must not disguise or conceal the identity of the sender.

Like the GDPR, the BDSG (New) also does not have any specific provisions regarding marketing. The use of electronic communication for the purpose of direct marketing is currently regulated in Art. 13 of the EU Directive 2002/58 which is implemented in Sec. 7 of the German Act Against Unfair Competition (*Gesetz gegen den unlauteren Wettbewerb* – 'UWG') which will remain unaffected by the BDSG and the GDPR, see Art. 95 GDPR. Both provisions will be replaced by Art. 16 of the ePrivacy Regulation (Regulation on Privacy and Electronic Communications). This will likely not change anything regarding marketing via electronic communications in Germany. According to a recent court decision, processing of personal data for the purpose of marketing communication which is in breach of Sec. 7 UWG also constitutes a breach of the GDPR as it does not follow a legitimate purpose (Administrative Court [*Verwaltungsgericht*] Saarlouis, decision dated 9 March 2018, case number 1 K 257/17).

For using electronic communication for direct marketing prior consent is necessary (Double-Opt-In process), Art. 16 (1), e-Privacy Regulation, Sec. 7 (2) no. 1, 2 UWG. According to Article 6 (1) lit. a GDPR as well as according to established German case law data subjects must always give consent for a specific processing purpose. This means that the person to

be contacted needs to know (1) from whom (meaning which specific entity) and (2) for which specific products and services he / she will receive marketing offers.

ONLINE PRIVACY

Traffic data

Traffic data qualifies as personal data. Providers of telecommunication services may collect and use the following traffic data to the following extent:

- the number or other identification of the lines in question or of the terminal
- authorisation codes, additionally the card number when customer cards are used
- location data when mobile handsets are used
- the beginning and end of the connection, indicated by date and time and, where relevant to the charges, the volume of data transmitted
- the telecommunications service used by the user
- the termination points of fixed connections, the beginning and end of their use, indicated by date and time and, where relevant to the charges, the volume of data transmitted, and
- any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes.

Stored traffic data may be used after the termination of a connection only where required to set up a further connection, for billing purposes or where the user has requested a connection overview.

The service provider may collect and use the customer data and traffic data of subscribers and users in order to detect, locate and eliminate faults and malfunctions in telecommunications systems. This applies also to faults that can lead to a limitation of availability of information and communications systems or that can lead to an unauthorized access of telecommunications and data processing systems of the users.

Otherwise, traffic data must be erased by the service provider without undue delay following termination of the connection.

Service providers have to inform the users immediately, if any faults of data procession systems of the users become known. Furthermore the service provider has to inform the users about measures for detecting and rectifying faults.

Location Data

Location Data qualifies as personal data. This data may only be processed as required for the provision of requested services and is subject to prior information of the user. For all other purposes, the user's informed consent must be obtained. According to Section 4a BDSG, 13 German Telemedia Act (TMG) this means that:

- the user's consent must be intentional, informed and clear. For this purpose the user must be informed on the type, the scope, the location and the purpose of data collection, processing and use including any forwarding of data to third parties
- the user's consent must be recorded properly
- the user must be able to access the content of his consent declaration any time. It is sufficient that such information is provided upon the users' request
- the user's consent must be revocable at all times with effect for the future.

Users must always be informed of the use of cookies in a privacy notice. Cookies may generally be used if they are required in order to perform the services requested by the user. Otherwise, users must be provided with an opt-out mechanism. For this purpose, information on the use of cookies together with a link on how to adjust browser settings in order to prevent future use is sufficient.

Germany has not yet taken any measures to implement the e-privacy directive. However, in February 2014 the German Federal Ministry of Economic declared that the European Commission considers the Cookie Directive as implemented in Germany. However, since the European Commission´s exact interpretation is not known, a final official clarification is awaited. It therefore remains to be seen whether an active opt in, e.g. by clicking on a pop up screen will be required in the future.

Different rules apply in the case of tracking technologies which collect and store a user's IP address. Since IP addresses qualify as personal data, their processing for tracking and marketing services requires active opt-in consent.

So far the German Tele-media Act (*Telemediengesetz* – 'TMG') applied for the purposes of online privacy. The Act stems from both data protection law and IT security law. The GDPR replaces all data protection related obligations from the TMG based on the Directive 95/46/EC. Solely the provisions Sec. 13 (1) sentence 2 TMG and Section 13 (7) TMG (which is based on Article 16 EU Directive on security of network and information systems (NIS Directive)) will still apply. As Sec. 13 (1) sentence 2 TMG does not correctly transpose Article 5 (3) Directive 2002/85/EC into German law, the German Authorities are of the opinion that the data protection rules of the BDSG are fully replaced by the GDPR. The German Authorities also have stated that online-tracking and profiling are only admissible with the data subject's consent. It remains to be seen whether this position will be upheld in court.

Commercial operators of tele-media services, which include website operators (even if services are provided for free), must, in the case of an automated procedure which permits subsequent identification of the recipient of the service and prepares the collection or use of personal data, inform the recipient of the service at the beginning of this procedure (Section 13 (1) sentence 2 TMG). Furthermore, they must take technical and organizational measures in light of 'state-of-the-art' technology to prevent security breaches and unauthorized access to their technical systems and to protect personal data (Section 13 (7) TMG).

KEY CONTACTS

Verena Grentzenberg
Of Counsel
T +49 40 1 88 88 208
verena.grentzenberg@dlapiper.com

Dr. Jan Geert Meents
Partner
T +49 89 23 23 72 130
jan.meents@dlapiper.com

Jan Pohle
Partner
T +49 221 277 277 391
jan.pohle@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

GHANA

Last modified 25 January 2017

LAW

Data Protection Act, 2012 (Act 843) ('Act').

DEFINITIONS

Definition personal data

Personal data is defined as:

- data about an individual who can be identified either:
  - from the data, or
  - from the data and other information in the possession of, or likely to come into the possession of the data controller.

Definition sensitive personal data

The Act does not make provision for 'sensitive personal data'. However 'special personal data', is defined as personal data which relates to:

- a child who is under parental control in accordance with the law, or
- the religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life or criminal behavior of an individual.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Commission ('Commission')

Room No. 51
First Floor
Ministry of Communications
Ministerial Enclave
P.O. Box CT 7195
Accra
Ghana

Tel: +233 302 631 455

REGISTRATION

A data controller who intends to process personal data is required to register with the Data Protection Commission. A data controller who is not incorporated in Ghana must register as an external company.

DATA PROTECTION OFFICERS

There is an obligation under the Act for data controllers to appoint data protection officers.

COLLECTION & PROCESSING

A person shall collect data directly from the data subject unless:

- the data is contained in a public record
- the data subject has deliberately made the data public
- the data subject has consented to the collection of the information from another source
- the collection of the data from another source is unlikely to prejudice a legitimate interest of the data subject
- the collection of the data from another source is necessary for a number of expressly designated purposes (for example the detection or punishment of an offence or breach of law)
- compliance would prejudice a lawful purpose for the collection
- compliance is not reasonably practicable.

A data controller must also ensure that the data subject is aware of:

- the nature of the data being collected
- the name and address of the person responsible for the collection
- the purpose for which the data is required for collection
- whether or not the supply of the data by the data subject is discretionary or mandatory
- the consequences of failure to provide the data
- the authorized requirement for the collection of the information or the requirement by law for its collection
- the recipient of the data
- the nature or category of the data
- the existence of the right of access to and the right to request rectification of the data collected before the collection.

Where collection is carried out by a third party on behalf of the data controller, the third party must ensure that the data subject has the information listed above.

TRANSFER

There are no specific provisions in the Act on the transfer of personal data. However, the sale, purchase, knowing or reckless disclosure of personal data or information is prohibited.

A person who knowingly or recklessly discloses personal data is liable on summary conviction to a fine of not more than 250 penalty units or to a term of imprisonment of not more than 2 years or to both. A person who sells or offers for sale personal data is liable on summary conviction to a fine of not more than 2500 penalty units or to a term of imprisonment of not more than five years or to both a fine and a term of imprisonment.

A penalty unit is equivalent to GHS12 (approximately USD $4.00).

SECURITY

A data controller is required to take steps to secure the integrity of personal data in the possession or control of a person through the adoption of appropriate, reasonable, technical and organisational measures to prevent:

- loss of, damage to, or unauthorised destruction
- unlawful access to or unauthorised processing of personal data.

BREACH NOTIFICATION

Where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by an unauthorised person, the data controller or a third party who processes data under the authority of the data controller shall notify the Commission and the data subject of the unauthorised access or acquisition as soon as reasonably practicable after the discovery of the unauthorised access or acquisition of the data. The data controller shall take steps to ensure the restoration of the integrity of the information system.

The data controller shall delay the notification to the data subject where the security agencies or the Data Protection Commission inform the data controller that the notification will impede a criminal investigation.

ENFORCEMENT

Where the Commission is satisfied that a data controller has contravened or is contravening any of the data protection principles, the Commission shall serve the data controller with an enforcement notice to require the data controller to do any of the following:

- to take or refrain from taking the steps specified within the time stated in the notice
- to refrain from processing any personal data or personal data of a description specified in the notice
- to refrain from processing personal data or personal data of a description specified in the notice for the purposes specified or in the manner specified after the time specified.

A person who fails to comply with an enforcement notice commits an offence and is liable on summary conviction to a fine of not more than one hundred and fifty penalty units or to a term of imprisonment of not more than one year or to both. A penalty unit is equivalent to GHS12 (approximately USD $4.00).

Further, an individual who suffers damage or distress through the contravention of the data protection obligations by a data controller is entitled to compensation from the data controller for the damage or distress notice.

ELECTRONIC MARKETING

The Act prohibits a data controller from using, obtaining, procuring or providing information related to a data subject for the purpose of direct marketing without the prior written consent of the data subject. However, there are no specific provisions that relate to electronic marketing specifically.

ONLINE PRIVACY

There are no specific provisions in relation to on-line privacy. However, a data controller is generally required to take necessary steps to secure the integrity of personal data in the possession or control of a person through the adoption of appropriate,

reasonable, technical and organizational measures.

KEY CONTACTS

Reindorf Chambers
www.reindorfchambers.com

Kizzita Mensah
T +233 302 225674/ 249564
kizzita.mensah@reindorfchambers.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

GIBRALTAR

Last modified 25 January 2017

LAW

A territory within the European Union (by virtue of the accession of the United Kingdom on 1 January 1973) Gibraltar implemented the EU data Protection directive 95/46 EC in 2006 with the Data Protection Act 2004 ('Act'). Enforcement is through the offices of the Data Protection Commissioner ('DPC').

DEFINITIONS

Definition of personal data

Any information relating to a Data Subject; and a Data Subject means a natural person who is the subject of Personal Data.

Definition of sensitive personal data

Information about racial or ethnic origin, religious or philosophical beliefs, trade union membership, health or sex life. The definition includes data regarding the commission or alleged commission of any offence and information on any proceedings for offences or alleged offences, the disposal of such proceedings and any sentence given.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Commissioner

Gibraltar Regulatory Authority
Suite 603 Europort
Gibraltar

T 200 74636
F 200 72166

info@gra.gi

REGISTRATION

Data controllers who process personal data must notify the Data Protection Commissioner by registering with the Gibraltar Regulatory Authority ('GRA') so that their processing of personal data may be registered and made public in the Data Protection Register, unless an exemption applies. Once registered any changes to the processing of personal data will require the Data Protection Register to be updated.

The notification must contain the following information:

- name and address of data controller and any representative
- description of the personal data being processed and the Categories to which they relate
- description of the purpose of the processing
- description of the recipients or categories of recipient to whom data will be sent
- names of any countries outside the EEA to which data is to be transferred to
- an adequate description of the security measures taken that is sufficient to allow a preliminary assessment of those measures, and
- other information reasonably required by the DPC.

DATA PROTECTION OFFICERS

There is no requirement in Gibraltar for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

- the data subject has unambiguously given his consent
- the processing is necessary for the performance of a contract to which the data subject is a party, or for actions to be carried out at the request of the data subject prior to entering into a contract
- the processing is necessary in order to comply with a legal obligation to which the data controller is subject
- the processing is necessary to prevent:
    - injury or other damage to the health of the data subject
    - serious loss or damage to his property
    - to protect his vital interests where seeking consent is likely to damage those interests
- the processing is necessary for a public purpose, namely:
    - for the administration of justice
    - for the performance of a statutory function
    - for the performance of a function of Government or of a Government Minister
    - the processing is necessary for the performance of a public function carried out in the public interest, and
    - the processing is necessary for upholding the legitimate interests of the data controller or of a third party to whom the data are supplied, except where the rights of the data subject under the European Convention of Human Rights and the Gibraltar Constitution prevail.

Where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of more stringent conditions.

TRANSFER

Data controllers may transfer personal data out of the EEA if any of the following conditions are met:

- the country to which the data is being transferred ensures an adequate level of protection by reference to statutory parameters
- the data subject consents to the transfer
- the transfer is necessary:
    - to perform a contract between the data subject and the data controller
    - to take steps at the request of the data subject in order to enter into a contract with the data controller
    - for the agreement or performance of a contract between a third party and the data controller at the request of the data subject
    - the transfer of data is required pursuant to an international obligation of Gibraltar; – the transfer is necessary due to a substantial public interest
    - the transfer is necessary to obtain legal advice either in respect of proceedings or to establish or defend a legal right
    - the transfer is necessary to protect the vital interests of the data subject, and
    - the transfer is made as part of personal data stored on a public register.

If none of these conditions are met, data outside of the EEA may still be transferred if:

- it is to a country approved by the EU commission as safe
- it is to a US organisation falling within the Safe Harbour provisions, or
- on terms incorporating the Model Clauses or approved Corporate Binding Rules. Alternatively the data controller can apply to the DPC for specific approval on a case by case basis.

SECURITY

Data controllers must take appropriate technical and organisational measures against accidental or unlawful destruction, loss or alteration of data, or against unauthorised disclosure or access to the information, and generally against all other unlawful forms of processing.

BREACH NOTIFICATION

There is currently no mandatory requirement in the Act to report data security breaches or losses to the DPC or to data subjects. A mandatory requirement will be introduced with the transposition into Gibraltar law of the Amendments to Directive 2002/58/EC (Directive on privacy and electronic communications) introduced by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

ENFORCEMENT

In Gibraltar, the DPC is responsible for the enforcement of the Act. If he becomes aware that the data controller is in breach of the Act, he can initiate proceedings against the data controller.

The ultimate sanction on conviction for an offence is a fine of GBP 4,000 (in the case of summary conviction in the magistrate's court) or GBP 10,000 (in the case of indictment in the Supreme Court).

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (eg an email address is likely to be 'personal data' for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to prevent the processing of their personal data (eg a right to 'opt out') for direct marketing purposes.

The Communications (PD&P) Regulations 2006 ('the Regulations') prohibit the use of automated calling systems without the consent of the recipient and unsolicited emails can only be sent without consent if:

- the contact details have been provided in the course of a sale or negotiations
- the marketing relates to a similar product or services, and
- the recipient was given a means of refusing the use of their contact details for marketing when they were collected.

Direct marketing emails must not disguise or conceal the identity of the sender in contravention of the E-Commerce Act. SMS marketing is also likely to be included within the prohibition on email marketing.

The restrictions on marketing by email only apply in relation to individuals and not where email marketing is sent to corporations.

ONLINE PRIVACY

The Regulations deal with the collection of location and traffic data by public electronic communications providers ('CPs') and the use of cookies (and similar technologies).

Traffic Data

Traffic Data held by a CP must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- it is being used to provide a value added service, and
- consent has been given for the retention of the Traffic Data.

Traffic Data can only be processed by a CP for:

- the management of billing or traffic
- dealing with customer enquiries
- the prevention of fraud
- the marketing of electronic communications services, or
- the provision of a value added service.

Location Data

Location Data may only be processed for the provision of value added services with consent and where the identity of the user is anonymised. CPs are also required to take measures and put a policy in place to ensure the security of the personal data they process.

Cookie Compliance

The use and storage of cookies and similar technologies requires:

- clear and comprehensive information, and
- consent of the website user.

Usual data protection principals of the Act also apply. Consent is not required for cookies that are used for the sole purpose of carrying out the transmission of a communication over an electronic communications network or where this is strictly necessary for the provision of a service requested by the user.

Enforcement of a breach of the Regulations is dealt with by the DPC and if found guilty a fine and or imprisonment may be imposed. However an individual may also bring an action for damages in the Supreme Court.

KEY CONTACTS

Hassans
www.gibraltarlaw.com/

Michael Nahon
Partner
T (+350) 200 79000
michael.nahon@hassans.gi

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

GREECE

Last modified 17 October 2018

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

A bill of law (the 'Bill') was published on February 20, 2018 which was submitted to public consultation. It should be noted that such Bill provides for both the legal measures implementing the Regulation 2016/679 (GDPR) in Greece, as well as the integration into the Greek legal order Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. However the Bill has not been enacted yet.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

Definition of supervisory authority

The supervisory authority is the Greek Data Protection Authority (hereinafter the Authority or the DPA) – under the reservation of Article 65 of the GDPR on the supervisory bodies of courts and public prosecutors.

Definitions as per article 4 of the GDPR

Such definitions are similar in the Bill, except for the definition of the public sector which substitutes the definition of 'international organization':

'Public sector' shall mean the national or public authorities, central and regional, independent public services, legal entities of public law, independent and regulatory administrative authorities, the national or public enterprises and organizations, the legal entities of private law belonging to the state or are subsidized from up to 50% of their annual budget at least or their management is defined by this, the local subsidiarity agencies of first and second instance as well as their legal entities and enterprises.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Data Protection Authority
1-3 Kifissias Avenue, Athens, 115 23 Greece.

T 2106475600
F 2106475628
contact@dpa.gr

The DPA is responsible for overseeing the Data Protection Law.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

There is no requirement in the Bill to notify / register with the DPA.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

Apart from the cases mentioned in Article 37 para. 1 of the GDPR, obligation of appointment of a data protection officer exists for data controllers or data processors which according to the list on all the processing operations issued by the DPA, which due to their nature, scope and / or purpose require regular and systemic monitoring of data subjects on a large scale.

Courts and Public Prosecutors offices are exempted from the obligation to appoint a DPO.

The appointment of the DPO must be made in writing and notified to the DPA.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the

accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Processing personal data

- Collection and processing of personal data for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller in accordance with the law.

- Processing of personal data for purposes different from those they have been collected for is permitted as long as:
  - it is strictly necessary in order to protect the vital interests of the data subject or of another natural person
  - it is strictly necessary for the performance of a task carried out in the public interest
  - it is strictly necessary for the establishment, exercise or defense of legal claims
  - it is necessary for the prevention, investigation, detection, confirmation or prosecution of criminal offences or the execution of criminal penalties
  - it is strictly necessary for national defense purposes

- Processing of personal data in the context of employment from an employer as data controller is allowed as long as:
  - it is necessary for the fulfillment of respective obligations related to the employment contract or deriving from the law or an individual or collective employment contract
  - it is necessary in order to comply with a legal obligation of the data controller
  - it is necessary in order to secure a vital interest of the employee as data subject or of another individual
  - it is necessary in order to fulfill the legal interest of the data controller or another third party, unless the legal interests or the fundamental rights and freedoms of the employee as data subject prevail

In the case that the data collection and processing is based on the consent of employees, such consent shall be written and distinguished from the employment contract. The employee shall have given his free and explicit consent and have the right to deny or withdraw his consent without negative impacts.

- Processing of special categories of personal data is allowed only as long as it is necessary for the exercise of specific rights and the performance of data controller or data subject obligations deriving from the contract of employment law, including obligations regarding employment security and safety, as well as social security law. It shall be carried out by the employer as data controller exclusively either for defined, explicit and legal purposes linked to the employment contract or for purposes deriving from legal provisions. Employees shall be informed beforehand about the processing purposes.

- The employer as data controller shall collect personal data from the data subjects. Collection of data regarding employee or candidate from third parties is allowed only as long as it is necessary for the fulfillment of legal purpose and the employee is informed beforehand about this collection. Personal data processed within the framework of employment relationship shall be appropriate, limited to the extent necessary for certain purposes related to the employment relationship 'data minimization'.

- Health data shall be collected directly and exclusively from the employees as long as it is absolutely necessary for a) employment assessment for a certain position, b) the fulfillment of employer's obligations regarding employment security and safety and c) establishment of employees' rights and social provisions offer. The performance of medical tests and analysis, such as psychological and psychometry tests, is allowed only in certain cases and as long as it is necessary for the specific job position. Processing of employee genetic data is prohibited, unless a legal clause explicitly sets out such procedure or it is necessary for protection of vital interests of the employees or third parties and upon consultation with the supervisory authority.

- The employer as data controller is entitled to process personal data regarding criminal convictions and offences, as well as security measures, as long as it is necessary for the employment assessment of an employee for a certain position or duties within the framework of the employment relationship.

- Collection and processing of biometric data within the framework of the employment relationship is allowed only if it is necessary for the protection of persons and goods.

- Processing of audiovisual data through CCTV (Article 6 of the GDPR) in order to protect individuals or / and goods.

  This clause covers the systems permanently established in a certain place that function constantly or for a regular period of time and have the ability to perceive or / and transmit audiovisual signals to a limited number of projection screens or/and recording machines. This clause does not apply to the following cases:

  - Non data processing activities, such as the functioning of simple access control systems without data recording
  - Activities in the course of a purely personal or household activity except for audiovisual processing through a CCTV system established in a private house, if the camera control scope includes public or common-shared spaces.

  Personal data shall be retained for no longer than is necessary for the purposes for which it is being processed. It shall be destroyed within 15 days at the latest unless more specific provisions applying to certain categories determine otherwise. In the case that an event relevant with the processing purposes arises, the data controller is allowed to keep the recoding containing this specific event in a separate file for a period of 3 months. After this period of time, the data controller may keep the data longer only in exceptional cases of further investigation of the event and under the obligation of informing the Authority about the necessary recording retention period.

- Collection and processing of personal data through CCTV within the workplace is allowed in special and

exceptional cases, as long as it is justified by the working conditions and scope and it is necessary for the protection of employees' health and security or working facilities. Such data shall not be used as exclusive criteria for behavior and efficiency assessment of employees.

The employer is obliged to draft a regulation governing the use of communication means and means of electronic processing in workplaces.

- Access to personal data kept **for archiving purposes** in the public interest is allowed as long as:
    - The data subjects have given their explicit consent
    - The processing is necessary in order to ensure vital interests of data subject or another individual
    - The processing is necessary for the fulfillment of a legal obligation carried out in the public interest in the exercise of official authority assigned to a third party who requests access to personal data
    - The processing is necessary for the establishment, exercise or defense of legal claims
    - The processing is necessary for scientific, historical or statistical purposes

In derogation from the provisions of Article 15 of the GDPR the access right of the data subject can be restricted in whole or in part to data related to it, if exercise of the right could possibly hinder the fulfillment of archiving purposes in the public interest, especially in the case that the archiving material is not kept in relation to the data subject's name and the exercise of the right would require disproportionate efforts.

In derogation from the provisions of Article 16 of the GDPR the data subject does not have the right of rectification of inaccurate data, if the exercise of this right could possibly hinder the fulfillment of archiving purposes in the public interest or the exercise of third parties' rights.

In derogation from the provisions of Articles 18, 19, 20 and 21 of the GDPR the data subject's rights are restricted, if these rights could possibly hinder the fulfillment of the specific archiving purposes in the public interest and such restrictions are considered as necessary for the fulfillment of those purposes.

- Processing of personal data for scientific, historical research purposes or statistical purposes is allowed as long as:
    - the data subjects have given their consent
    - the data controller already has such data from previous research and the data subjects have given their consent to further use or use for relevant purposes
    - The personal data derive from public accessible sources
    - The data controller can prove that the processing is necessary for scientific or historical research purposes or statistical purposes and the data subjects rights do not prevail

Processing sensitive personal data / consent

Articles 7, 8, 9, 10 of the GDPR

- Processing of health data must be based on the explicit and written consent of the data subject.

- Collection and processing of genetic data or / and preventive genetic diagnosis carried out for health and life insurance purposes is prohibited. Such processing is also prohibited for the data subject family members.

- Processing of personal data relating to criminal convictions and offences is permitted, if it is strictly necessary for the purpose of one of the following:
    - Recruitment and assessment for job positions
    - Employment relations under the certain preconditions and guarantees of article 17
    - Archiving in the public interest, scientific or historical research or statistics in accordance with articles 18 and 19
    - Academic, artistic, literary and journalistic expression in the scope of freedom of expression and information
    - Establishment, exercise and defense of legal claims

Processing of personal data relating to criminal convictions and offences is permitted upon the explicit and written consent of the data subject, if it is necessary to take measures requested by the data subject, such as reintegration. Furthermore, the processing of those personal data in the scope of academic, artistic, literary as well as journalistic purposes shall be the adequate, relevant and limited to secure the freedom of expression and the right to information ('data minimisation').

Processing of sensitive personal data, as well as those relating to criminal convictions and offences for scientific or historical research purposes or statistical purposes is allowed in the following cases:

- The data subject has given its prior explicit consent. In cases of clinical trials for scientific purposes the provisions of Art. 28-34 of the Regulation 536/2014 are also applicable
- The data controller has access to those data from previous relevant scientific or statistical research activities and the data subjects have given consent to further use
- The data controller is able to prove that the processing is necessary for scientific or historical research purposes or statistical purposes which do not override the rights of the data subjects.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The transfer of personal data is permitted:

- in order to protect the vital interests of the data subject or another natural person
- for substantial public interest reasons and
- for the establishment, exercise or defence of legal claims

after having provided the data subject with information regarding this purpose as well as all the essential information as specified in article 14 of the GDPR.

The transfer of personal data deriving from a CCTV system to third parties is permitted in the following cases:

- after prior explicit consent of the data subject
- in exceptional cases, after justifiable request of a third party, when the data is necessary to be used as evidence for the establishment, exercise or support of legal claims or crimes

The transfer of personal data to courts, public prosecutors and policy authorities upon request, in the exercise of their legal obligations, is not regarded as transfer to third parties.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The processing of personal data must be confidential. It must be carried out solely and exclusively by persons acting under the authority of the data controller or the processor and upon his instructions.

In order to carry out data processing, the data controller must choose persons with corresponding professional qualifications providing sufficient guarantees in respect of technical expertise and personal integrity to ensure such confidentiality.

The data controller must implement appropriate organizational and technical measures (TOMs) to secure data and protect it against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access as well as any other form of unlawful processing. Such measures must ensure a level of security appropriate to the risks presented by processing and the nature of the data subject to processing.

If the data processing is carried out on behalf of the data controller, by a person not dependent upon him, the relevant assignment must be in writing. Such assignment must provide that the processor carries out such data processing only on

instructions from the data controller and that all other confidentiality obligations must mutatis mutandis be borne by him.

Before a person enters the scope of a CCTV system, the controller must inform in an appropriate and clear way about the CCTV system, the processing purpose, the establishment place, as well as the time for which the personal data will be retained.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

As provided in Articles 30 and 31 of the GDPR

In case of a breach of personal data, the data controller is obliged to notify the DPA within 72 hours as of the moment he is aware of such breach. The data processor needs to immediately notify the data controller of any breach he become aware.

Specific details must be included in the notification form on the nature of the breach, the categories of the data the repercussions of the breach and whether the data has been transferred to another Member State.

The notification of a personal data breach to the data subject shall not be performed if the data processing relates to one of the following purposes:

- national security
- national defense
- public security
- prevention, investigation or prosecution of criminal convictions and offences, including the protection from and prevention of threats against public security
- important economic or financial state interests including monetary, financial and tax, public health as well as social insurance issues, especially regarding performance of relevant audits
- establishment, exercise or defense of legal claims, and
- the breach notification would be harmful for the fulfilment of those purposes

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Administrative fines

The DPA may impose administrative fines in accordance with article 83 para. 4 and 5 of the GDPR. The acts of the DPA through which administrative fines are imposed, constitute enforceable deeds and shall be served to the data controller, the data processor or their representatives. Such fines shall be collected according to the Public Income Collection Code.

Penalties

As provided by for Article 84 of the GDPR and namely:

- Anyone unlawfully interfering in any way whatsoever with a personal data file or takes note of such data or extracts, alters, affects in a harmful manner, destroys, processes, transfers, discloses, makes accessible to unauthorized persons or permits such persons to take notice of such data or anyone who exploits such data in any way whatsoever, will be punished by imprisonment.
- If the above mentioned actions refer to special categories of data or data relating to criminal prosecutions, security measures as well as criminal convictions, the perpetrator will be punished by imprisonment for a period of at least one year and a fine amounting between 10.000 Euros and 100.000 Euros, unless otherwise subject to more serious sanctions.
- If the perpetrator of the above mentioned actions acts in order to provide himself or someone else with an unlawful asset, cause pecuniary damage or harm someone else, he will be punished by imprisonment for a period of at least three years and a fine amounting between 100.000 Euros and 300.000 Euros, unless otherwise subject to more serious sanctions.
- If the perpetrator has caused a danger for the free function of the democratic regime or the national security through the above mentioned actions, will be punished by incarceration and a fine of between 100.000 Euros and 300.000 Euros.
- Any data protection officer who infringes the confidentiality obligation in the scope of occupational privacy by announcing or revealing facts or information, which it has been aware of through the exercise of its tasks, in order to benefit itself or a third party or harm the controller, the processor, the data subject or a third party, will be published by imprisonment for a period of time of at least 1 year and a fine of between 10.000 Euros and 100.000 Euros, unless otherwise subject to more serious sanctions.
- All the above mentioned actions shall be prosecuted only following the filing of a criminal complaint.
- The felonies fall under the jurisdiction of the Three-Member Felony Court of Appeals.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the

strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Electronic marketing is regulated by Law 3471/2006 'for the protection of personal data and privacy in electronic communications' (the 'Law'), in combination with the general provisions of Law 2472/1997 *'for the protection of individuals from the processing of personal data'* (the 'Data Protection Act').

According to the provisions of article 11 of the Law, data processing for electronic marketing purposes is allowed only upon the individuals' prior express consent. The said article prohibits the use of automated calling systems for marketing purposes to subscribers that have previously declared to the public electronic communications services providers ('CSPs') that they do not wish to receive such calls in general. The CSPs must register these declarations for free on a separate publicly accessible list.

Personal data (such as e-mail addresses) that have been legally obtained in the course of sales of products, provision of services or any other transaction may be used for electronic marketing purposes, without the receiver's prior consent thereto, provided that the receiver of such email has the possibility to 'opt out' for free to the collection and processing of his/ her personal data for the aforementioned purposes.

Direct marketing emails or advertising emails of any kind are absolutely prohibited, when the identity of the sender is disguised or concealed and also when no valid address, to which the receivers can address requests for the termination of such communications, is provided.

Electronic marketing is regulated by Law 3471/2006 'for the protection of personal data and privacy in electronic communications' (the 'Law'), in combination with the general provisions of the General Data Protection Regulation (Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data).

According to the provisions of article 11 of the Law, data processing for electronic marketing purposes is allowed only with the individuals' prior express consent. The said article prohibits the use of automated calling systems for marketing purposes to subscribers that have previously declared to the public electronic communications services providers ('CSPs') that they do not wish to receive such calls in general. The CSPs must register these declarations for free on a separate publicly accessible list.

Personal data (such as e-mail addresses) that have been legally obtained in the course of sales of products, provision of services or any other transaction may be used for electronic marketing purposes, without the receiver's prior consent thereto, provided that the receiver of such email has the possibility to 'opt out' for free to the collection and processing of his/ her personal data for the aforementioned purposes.

Direct marketing emails or advertising emails of any kind are absolutely prohibited, when the identity of the sender is disguised or concealed and also when no valid address, to which the receivers can address requests for the termination of such communications, is provided.

ONLINE PRIVACY

Articles 4 and 6 of the Law (as amended by Directive 2009/136/EC) deals with the collection of location and traffic data by CSPs and the use of cookies and similar technologies.

Traffic data

Traffic data of subscribers or users held by a CSP must be erased or anonymized after the termination of a communication, unless they are retained for one the following reasons:

- The billing of subscribers and the payment of interconnections, provided that the subscribers are informed of the categories of traffic data that are being processed and the duration of processing, which must not exceed 12 months from the date of the communication (unless the bill is doubtable or unpaid).

- Marketing of electronic communications services or value added services, to the extent that traffic data processing is absolutely necessary and following the subscriber's or the user's prior express consent thereto, after his / her notification regarding the categories of traffic data that are being processed and the duration of the processing. Such consent may be freely recalled. The provision of electronic communication services by the CSP must not depend on the subscriber's consent to the processing of his/her traffic data for other purposes (*eg,* marketing purposes).

Location data

Location data may only be processed for the provision of value added services, only if such data are anonymized or with the subscriber's / user's express consent, to the extent and for the duration for which such processing is absolutely necessary. The CSP must previously notify the user or the subscriber of the categories of location data that are being processed, the purposes and the duration of the processing as well as of the third parties to which the data will be transmitted for value added services provision. The subscriber's / user's consent may be freely recalled and the 'opt-out' possibility must be provided to the subscriber by the CSP free of charge and with simple means, every time he is connected to the network or in each transmission of communication.

Location data processing is allowed exceptionally without the subscriber's / user's prior consent to authorities dealing with emergencies, such as prosecution authorities, first aid or fire-brigade authorities, when the location of the caller is necessary for serving such emergency purposes.

Cookie compliance

The use and storage of cookies and similar technologies is allowed when the subscriber / user has provided his express consent, after his / her comprehensive and detailed notification by the CSP. The subscriber's consent may be provided through the necessary browser adjustments or through the use of other applications.

The latter do not prevent the technical storage or use of cookies for purposes relating exclusively to the transmission of a communication through an electronic communications network or the provision of an information society service for which the subscriber or the user has specifically requested. The Data Protection Authority is the competent authority for the issuance of an Act, which will regulate the ways such services will be provided and the subscribers' consent will be declared.

Traffic data of subscribers or users held by a CSP must be erased or anonymized after the termination of a communication, unless they are retained for one the following reasons:

- The billing of subscribers and the payment of interconnections, provided that the subscribers are informed of the categories of traffic data that are being processed and the duration of processing, which must not exceed 12 months from the date of the communication (unless the bill is doubtable or unpaid).

- Marketing of electronic communications services or value added services, to the extent that traffic data processing is absolutely necessary and following the subscriber's or the user's prior express consent thereto, after his / her notification regarding the categories of traffic data that are being processed and the duration of the processing.

Such consent may be freely recalled. The provision of electronic communication services by the CSP must not depend on the subscriber's consent to the processing of his / her traffic data for other purposes (*eg,* marketing purposes).

Location data

Location data may only be processed for the provision of value added services, only if such data are anonymized or with the subscriber's / user's express consent, to the extent and for the duration for which such processing is absolutely necessary. The CSP must previously notify the user or the subscriber of the categories of location data that are being processed, the purposes and the duration of the processing as well as of the third parties to which the data will be transmitted for value added services provision. The subscriber's / user's consent may be freely recalled and the 'opt-out' possibility must be provided to the subscriber by the CSP free of charge and with simple means, every time he is connected to the network or in each transmission of communication.

Location data processing is allowed exceptionally without the subscriber's/user's prior consent to authorities dealing with emergencies, such as prosecution authorities, first aid or fire-brigade authorities, when the location of the caller is necessary for serving such emergency purposes.

Cookie compliance

The use and storage of cookies and similar technologies is allowed when the subscriber / user has provided his express consent, after his/her comprehensive and detailed notification by the CSP. The subscriber's consent may be provided through the necessary browser adjustments or through the use of other applications.

The latter does not prevent the technical storage or use of cookies for purposes relating exclusively to the transmission of a communication through an electronic communications network or the provision of an information society service for which the subscriber or the user has specifically requested. The Data Protection Authority is the competent authority for the issuance of an Act, which will regulate the ways such services will be provided and the subscribers' consent will be declared.

KEY CONTACTS

Kyriakides Georgopoulos Law Firm
www.kglawfirm.gr

Effie Mitsopoulou
Partner
T +30 210 817 1540
e.mitsopoulou@kglawfirm.gr

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

GUERNSEY

Last modified 28 January 2019

LAW

The Data Protection (Bailiwick of Guernsey) Law 2017 (DPL 2017) came into force on May 25, 2018 to coincide with the enforcement of the EU's General Data Protection Regulation (EU) 2016/670 (GDPR).

Adequacy:

The DPL 2017 replaced Guernsey's previous data protection legislation, the Data Protection (Bailiwick of Guernsey) Law, 2001 as amended (DPL 2001) which was implemented in response to Directive 95/46/EC. Unlike the DPL 2001, the DPL 2017 is not modeled after a UK enactment. It is, however, stated to be equivalent to the GDPR.

In 2003, Guernsey was recognized by the European Commission as providing an adequate level of protection for free flow of personal data to the Bailiwick (see Opinion 02072/07/EN WP 141 and Opinion 10595/03/EN WP 79). This decision remains in place for the purposes of the GDPR until it is reassessed by the European Commission on or around 2020 (as per Article 45(9) GDPR).

Scope and Applicability:

The DPL 2017 applies in relation to the processing of personal data where both of the following conditions are met:

- The processing is by automated means (whether wholly or partly) or if the processing is not by automated means it is intended to form part of a filing system
- The processing is conducted by a controller or processor established in the Bailiwick of Guernsey ("Bailiwick") or the personal data is that of a Bailiwick resident and is processed in the context offering goods or services (whether or not for payment) to the resident or the monitoring of a resident's behavior in the Bailiwick

In practice, this means that there may be instances where controllers and processors established in the Bailiwick are subject to both the DPL 2017 and, where they process personal data of data subjects who are in the EU, the GDPR.

However, unlike the GDPR, the Data Protection (Commencement, Amendment and Transitional) (Bailiwick of Guernsey) Ordinance, 2018 (DP Ordinance), provides controllers and processors with limited transitional relief from certain areas of the DPL 2017 (Transitional Provisions). This means that controllers and processors who are subject to the DPL 2017 have until May 25, 2019 to ensure compliance for certain duties. This includes relief from the duty to:

- Notify pre-collected data
- Carry out privacy impact assessments
- Comply with statutory obligations in connection with certain processor and joint controller-led duties

- Renew consents where they have been validly obtained before May 25, 2018

In reality, the Transitional Provisions only provide limited comfort to those controllers and processors who process personal data of Bailiwick residents only. Where an organization is subject to the GDPR, then it must, notwithstanding the Transitional Provisions, comply with all aspects of the GDPR.

DEFINITIONS

Definition of personal data

Section 111(1) of the DPL 2017 defines personal data as any information relating to an identified or identifiable individual.

An identifiable individual is given special meaning under Schedule 9 of the DPL 2017 and is defined as an individual who can be directly or indirectly identified from the information including:

- By reference to a name or an identifier
- One or more factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity
- Where, despite pseudonymization, that information is capable of being attributed to that individual by the use of additional information
- By any other means reasonably likely to be used, taking into account objective factors such as technological factors and the cost and amount of time required for identification in the light of the available technology at the time of processing

Definition of sensitive personal data

Special category data means personal data consisting of information as to a data subject's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data, meaning personal data relating to the inherited or acquired genetic characteristics of an individual which gives unique information about their physiology or their health, including as a result of an analysis of a biological sample from that individual
- Biometric data, meaning personal data resulting from the specific technical processing relating to the physical, physiological or behavioral characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data
- Health data, which includes any personal data relating to the health of an individual, including the provision of health care services, which reveals their health status and includes information about their physical or mental health
- Sex life or sexual orientation
- Criminal data which relates to the commission or alleged commission by an individual of any offense, or any proceedings for any offense committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

NATIONAL DATA PROTECTION AUTHORITY

Overall oversight of the implementation of the DPL 2017 is vested in a new independent body, the Data Protection Authority (the

Authority). The DP Authority delegates many of the day-to-day regulatory functions and provides governance to an independent operational body known as the Office of the Data Protection Authority (ODPA) (formerly, the Office of the Data Protection Commissioner).

The DP Authority and the ODPA are also required, pursuant to The Data Protection (International Cooperation and Assistance) (Bailiwick of Guernsey) Regulations, 2018 to have regard to Articles 60 – 62 GDPR by providing mutual cooperation with other supervisory authorities relating to both the GDPR and the DPL 2017.

The Office of the Data Protection Authority

St Martin's House
Le Bordage, St. Peter Port
Guernsey GY1 1BR

T: +44 (0) 1481 742074
E: enquiries@odpa.gg

W: https://odpa.gg

REGISTRATION

Schedule 4 of the DPL 2017 requires all controllers and processors established in the Bailiwick to register with the ODPA. The DP Authority may prescribe the form and manner of registration.

Guidance (*Notification and Registration*) confirms that the DPL 2017 will maintain a similar reporting requirement. Therefore, any information (including fees) that was necessary in respect of the DPL 2001 is still required under the new regime, in addition to a small number of areas such as contact details for data protection officers (as applicable):

- The name and address of the data controller
- The name and address of any nominated representatives
- A description of the data and the category or categories of data subject to which they relate
- Why the information is processed
- A description of any recipient or recipients to whom the data controller intends or may wish to disclose the data
- The names, or a description, of any countries or territories outside the Bailiwick of Guernsey to which the data controller directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the data

The notification must also contain a general description of the measures to be taken to prevent unauthorized or unlawful processing of, accidental loss or destruction of, or damage to, personal data.

Registered entities or persons are required to notify the ODPA of any changes to the registered details.

The Transitional Provisions extend to registration requirements until May 25, 2019. This means that those controllers who were exempted from registration under the 2001 Law have until May 25, 2019 to ensure that they have the requisite processes in place to enable them to comply with their registration requirements.

A new registration system is due to be implemented by May 25, 2019 to coincide with a new regulatory regime governing the levying of fees. At the time of writing, we understand that the DP Authority has submitted its proposals for consultation with the States of Guernsey and further guidance is anticipated in Spring 2019.

DATA PROTECTION OFFICERS

A data protection officer (DPO) must be appointed where either of the following apply:

- Processing is carried out by a public authority (other than a court, or tribunal acting in a judicial capacity)
- The core processing operations of the controller or processor require or involve large-scale and systematic monitoring of data subjects or large-scale processing of special category of data

The ODPA has issued guidance clarifying what is intended by the use of the term large-scale processing which is neither defined in the GDPR nor the DPL 2017.

With reference to guidance issued by Europe's former advisory body known as the Article 29 Working Party (now replaced by the European Data Protection Board (EDPB) on the appointment of DPOs ("DPO Guidelines"), the ODPA's guidance advises controllers and processors to take into account the terms of the GDPR and the DPO Guidelines when assessing whether a DPO is required to be appointed. It further clarifies that small businesses in Guernsey are, as a general rule, unlikely to be undertaking large-scale processing unless they work with large databases of customers or other types of data subjects. The ODPA expects controllers and processors to review the scope and nature of processing periodically to ascertain whether there are sufficient factors to warrant appointing a DPO. All controllers and processors should then document the outcome of such reviews.

COLLECTION & PROCESSING

Principles

Data controllers must comply with the following data protection principles set out under Section 6(2) DPL 2017 ("Principles"):

- **Lawfulness, fairness and transparency**: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data
- **Purpose limitation**: personal data must be collected for specified, explicit and legitimate purposes and once collected, not further processed in a manner incompatible with those purposes
- **Data minimization**: personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- **Accuracy**: personal data must be accurate and, where necessary, kept up to date, with reasonable steps being taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- **Storage limitation**: personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed
- **Integrity and confidentiality**: personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures
- **Accountability**: the controller is responsible for, and must be able to demonstrate, compliance with all other data protection principles

Lawful basis

Data controllers are required to ensure that they have a lawful basis for processing personal data. The DPL 2017 sets out a number of conditions which may be relied upon to legitimize the processing of personal data and special category data.

The most common conditions for controllers to rely on are:

- The data subject consents to the processing
- The processing is necessary for the performance of a contract to which the data subject is a party or between a controller

and a third party in the interests of a data subject; or in order to take steps at the data subject's request with a view to entering into a contract

- The processing is necessary for the controller to exercise any right or power, or perform or comply with a duty imposed on it by law, otherwise than an obligation imposed by an enactment, an order, or a judgment of a court or tribunal having the force of the law in the Bailiwick
- The processing is necessary in order to protect the vital interests of the data subject
- The processing is necessary for legitimate interests of the controller or third party except where the processing is exercised by a public authority
- The processing is necessary for the exercise or performance by a public authority of a function that is of a public nature or a task carried out in the public interest

In addition to these conditions, controllers may also rely on one or more of a restrictive set of conditions in order legitimize either personal data or special category data. These include (but are not limited to):

- Data subject providing *explicit* consent to the processing
- Processing which is necessary for compliance with a legal right or power or duty imposed on a controller by an enactment
- Processing which is made public as a result of steps deliberately taken by the data subject
- Processing which is necessary for the purpose of or in connection with legal proceedings, the discharge of any functions of a court or tribunal, obtaining legal advice or establishing, exercising or defending legal rights
- Processing which is the administration of justice of the exercise of any function of the Crown, the States of Guernsey or a public committee
- Processing which is necessary for a historical or scientific purpose
- Processing for the vital interests of a data subject

For the purposes of Section 10 DPL 2017, where a controller seeks to rely on consent, the controller must comply with more stringent requirements than under the DPL 2001 in order to ensure that such consent is valid.

Valid consent must be (among others) a "specific, informed and unambiguous indication of the data subject's wishes by which a data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of their personal data." In this regard, the DPL 2017 sets the same high standards for consent as the GDPR.

Guidance issued by the ODPA clarifies that in addition to the ingredients required to achieve valid consent, explicit consent must also be expressly confirmed in words, rather than a positive action. The requirements are summarized in a checklist for controllers to rely on when relying on consent.

Finally, Section 10(2)(f) DPL 2017 stipulates that a child may only provide their own consent to processing in respect of information society (primarily, online) services, where that child is over 13 years of age. Otherwise a parent (or other responsible adult) must give it on their behalf.

Transparency

Requirements of transparency under the DPL 2017 closely align with the GDPR. Therefore, the DPL 2017 requires that certain specified information must be supplied as part of a fair processing notice. (Schedule 3 DPL 2017):

- The identity and contact details of the controller, and (where applicable), the controller's representative
- The contact details of the data protection officer (if any)

- Confirmation of whether any of the personal data is special category data
- Where the personal data are not obtained directly from the data subject: confirmation of the source of the personal and (if applicable) confirmation whether the personal data was obtained from a publicly available source confirmation of the source
- The purposes for which the data are intended to be processed and the legal basis for the processing
- An explanation of the legitimate interests pursued by the controller or by a third party, if the processing is based on those interests
- The recipients or categories of recipients of the personal data (if any)
- Where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and whether or not there is an adequate level of protection for the rights and freedoms of data subjects
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- Information concerning the rights of data subjects
- Where the processing is based on consent, the existence of the right to withdraw consent
- A statement of the right to complain to the DP Authority
- The existence of any automated decision-making and any meaningful information about the logic involved in such decision-making and the significance of any such decision-making for the data subject
- Any further information that is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair

Rights of the Data Subject

The DPL 2017 has strengthened the rights of data subjects in line with the GDPR (Part III DPL 2017).

Controllers must respond to a request "*as soon as practicable*" and in any event within one month following receipt of the request or receipt of the information necessary to confirm the identity of the requestor or the day on which a fee or charge is paid to the controller.

The following rights are available to data subjects:

- ***Right to information for personal data collected about the data subject either directly or indirectly (Sections 13 – 14 DPL 2017)***: Where personal data has been collected from a source other than the data subject, certain exceptions are available.
- ***Right to data portability (Section 15 DPL 2017):*** A data subject has the right to have certain *relevant* personal data (being personal data relating to that person which has been provided to the original controller directly or via a processor) ported to a new controller, where either:
    - That relevant personal data is being processed based on consent
    - The processing necessary for the conclusion or performance of a contract
    - Where the right applies, the original controller must ensure that any personal data transmitted is provided in a structure, commonly used and machine-readable format. The right is subject to certain exceptions set out under Section 16 DPL 2017.
- ***Right of access (Section 15 DPL 2017)*:** A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about how the data has been used by the controller. Section 16 DPL

2017 provides for certain exceptions, including where a request cannot be complied with, without disclosing information about another individual balancing the rights of the requestor with significant interests of the other individual. The DPL 2017 sets out further detail in respect of the factors which should be taken into consideration when making this determination.

- ***Right to object to processing (Section 17 – 19 DPL 2017):*** Data subjects have the right to object to processing for: (a) direct marketing purposes, (b) on public interest grounds and (c) where the processing is for historical or scientific purposes. While the right to object in respect of paragraph (a) is unconditional, the rights to object under paragraphs (b) and (c) are qualified and subject to a public interest tests.

- ***Right to rectification (Section 20 DPL 2017*)**: A data subject has a right to request that any inaccurate or incomplete personal data may be corrected or a statement on the controller's file noting that the data subject disputes the accuracy or completeness of the personal data.

- ***Right to erasure (Section 21 DPL 2017)*:** Data subjects may request erasure of their personal data. The right is not absolute: it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or following the successful exercise of the objection right, or of the withdrawal of consent.

- ***Right to restriction of processing (Section 22 DPL 2017*)**: A data subject may request that the processing of their personal data is restricted in certain limited circumstances. For example: where the accuracy of the personal data is contested; where the processing is unlawful; where the data is no longer required (save for legal claims or for the purposes of obtaining legal advice or establishing/exercising or defending legal rights).

- ***Right to notified of restriction, erasure or rectification (Section 23 DPL 2017)*:** The controller must not only notify the data subject concerned but, unless it is impracticable or involves disproportionate effort, notify any other person whose personal data has been disclosed.

- ***Right not to be subject to decisions based on automated processing (Section 24 DPL 2017)*:** A data subject has a right not to be subjected to an automatic decision and a controller is prohibited from causing or permitting a data subject to be subjected to an automatic decision unless Section 24(2) DPL applies.

  This section permits automated processing where: the data subject has given their explicit consent, or it has been authorized by the States of Guernsey or via an enactment; or the automated processing is necessary for: the vital interests of the data subject or another person; for the performance of a contract.

  Additional restrictions apply for the automated processing of special category data. A controller must ensure that appropriate safeguards are in place where automated processing has been conducted in accordance with Section 24(2) DPL (including allowing the data subject to appeal or seek a review of the decision).

- ***Right to make a complaint to ODPA (Section 67 DPL 2017)*:** a data subject may also complain in writing to the ODPA if they consider that a controller or processor has breached or is likely to breach the DPL 2017 and that breach involves or affect (or likely to involve or affect) personal data relating to the individual or any data subject right of the individual.
- ***Right to bring a civil action against a controller or processor for breach duty (Section 79 DPL 2017)*:** where a controller or processor breaches an operative provision under the DPL 2017 that causes damage to another person, the injured party may bring a tortious claim in court against the controller or processor for breach of statutory duty. The court may award damages, an injunction to restrain actual/anticipated breach of duty and make a declaration that the controller or processor has committed the breach or will commit a breach if its current course of action subsists. Individuals may also claim compensation for distress, inconvenience or other adverse effect suffered by an injured party even if it does not result from any physical or financial loss or damage. Group (or 'class') actions may also be brought against an organization (Section 97 DPL 2017).

TRANSFER

The DPL 2017 differentiates between *authorized jurisdictions* and *unauthorized jurisdictions*.

Authorized jurisdictions include the Bailiwick of Guernsey, a member state of the European Union, any country, sector or international organization which has been determined by the European Commission as providing an '*adequate level of protection*' for the rights and freedoms of data subjects; or any designated jurisdiction. A designated jurisdiction includes the UK (or any country within the UK), any crown dependency or any sector within the UK or a crown dependency.

Unauthorized jurisdictions mean any countries, sectors in a country or international organization that does not fall within the scope of an authorized jurisdiction.

Personal data must not be transferred outside of the Bailiwick of Guernsey by a controller or processor ("Exporter") to an unauthorized jurisdiction unless the Exporter is satisfied that any of the following conditions are satisfied:

- Particular safeguards are in place and there is a mechanism for data subjects to enforce their rights and obtain effective legal remedies against controller or processor receiving the personal data ("Importer") (section 56 DPL 2017)
- The DP Authority or the ODPA has authorized the transfer (section 57 DPL 2017)
- Other specified derogations exist (section 59 DPL 2017)

Safeguards, for the purposes of the first condition named above, include: legally enforceable agreements (where the Importer is a public authority/body), binding corporate rules, EU's Model Clauses (or equivalent provisions as may from time to time be in force) or approved codes or other approved mechanisms which combine binding and enforceable commitments on the Importer.

While the DPL 2017 does not expressly reference the EU-US Privacy Shield and the ODPA has not yet issued updated guidance in relation to international transfers under the DPL 2017, it is likely that, for so long as the Privacy Shield framework remains operational, Privacy Shield will be recognized as an approved mechanism for transferring personal data to the United States.

Derogations include:

- The data subject has given explicit consent to the transfer after having been informed of the risks of the transfer
- The transfer is necessary for the performance of a contract between the data subject and the controller or between the controller and third party in the interests of the data subject or for the taking of steps at the request of the data subject with a view to the data subject entering into a contract with the data controller
- The transfer is authorized by regulations made for reasons of public interest
- The transfer is necessary for, or in connection with, legal proceedings, obtaining legal advice or for the purposes of establishing, exercising or defending legal rights
- The transfer is necessary to protect the vital interests of the data subject or another individual (provided that the data subject is physically or legally incapable of giving consent or the controller cannot be reasonably expected to obtain explicit consent)
- The transfer is part of personal data on a public register or a register to which a member of the public has lawful access
- A decision of a public authority (within or without the Bailiwick) based on international agreement imposing international obligations on the Bailiwick or an order of a court or tribunal
- The transfer is in the legitimate interests of the controller which outweighs the significant interests of the data subject and the transfer is:
    - Not repetitive
    - Only concerns a limited number of data subjects
    - Controller has assessed all circumstances surrounding the data transfer and on the basis of assessment has provided appropriate safeguards to protect personal data

Where the transfer is legitimized on the legitimate interests grounds described above, both the ODPA and the data subject must be notified accordingly.

SECURITY

Security appears more prominently under the DPL 2017 than its predecessor. While implementing appropriate security measures to safeguard personal data from unauthorized or unlawful processing continues to be a feature of the DPL 2017 (see Principle 6 'Integrity and Confidentiality'), the DPL 2017 (unlike its predecessor) sets out with more clarity the steps required to ensure compliance.

Data controllers must take reasonable steps to ensure a level of security which is appropriate to the personal data, taking into account the nature, scope, context and purpose of the processing, the likelihood and severity of the risks to data subjects if the personal data is not secure (including the risk of unlawful or accidental destruction, loss or alteration of personal data and unauthorized disclosure of personal data), best practices and the costs of implementing appropriate measures.

Section 41 of the DPL 2017 provides clarity as to what a required 'step' would constitute. In essence, to ensure compliance with this obligation, a controller should consider this following:

- Pseudonymizing and encrypting personal data
- Ensuring that the controller or processor has and retains the ability to do the following:
    - Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
    - Restore access to personal data in a timely manner in the event of a physical or technical incident
- Establishing and implementing a process for regular testing and evaluation of the effectiveness of the technical and organizational measures

The security obligations are strewn throughout the DPL 2017 and not only appear on account of Part VI of the DPL 2017 but are also a key consideration when undertaking a data protection impact assessment, the right to erasure, a controller's duty to take reasonable steps to achieve compliance and what measures are in place when choosing a processor. For example, in this regard, a controller must when assessing the suitability of a processor ensure that the processor provides (in addition to a data processing agreement) sufficient guarantees that reasonable technical and organizational security measures governing the processing to be carried out will be established and carried out to meet the requirements of the DPL 2017 and will safeguard the rights of data subjects.

BREACH NOTIFICATION

What is a breach?

The DPL 2017 defines a personal data breach as a "breach of security leading to the a) accidental or unlawful destruction, loss, or alteration of; or b) unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise process."

This definition replicates the definition under Article 4 of the GDPR.

Notice to ODPA:

As with the GDPR, the DPL 2017 requires all controllers, upon becoming aware of a personal data breach to provide written notice to the ODPA as soon as practicable and no later than 72 hours after becoming so aware. Section 42(5) of the DPL 2017 provides an exemption from the duty to notify the ODPA where the personal data breach is "unlikely to result in any risk to the significant interests of the data subject."

In determining whether there is a risk, the ODPA's guidance entitled *Notification of Personal Data Breaches* ("Breach Guidance") advises organizations who process personal data to consider the type of personal data they hold and whether any breach could, both at the time of the breach and in the future, 'adversely affect an individual' taking into consideration financial loss, reputational

damage, or identity fraud.

The DPL 2017 stipulates the types of information which must be provided to the ODPA include, a description of the nature of the personal data breach, contact details of the DPO or contact point, a description of the likely consequences of such a breach, a description of the measures taken or proposed to be taken to address risks and mitigate against possible adverse effects and an explanation of any delays (where a breach has been notified after 72 hours).

All breaches which must be notified to the ODPA can be submitted to the ODPA via their online secure breach reporting facility. All breaches that come to the attention of the controller after May 25, 2018 must be reported to the ODPA, regardless of when they occurred.

In any case, whether a personal data breach is notified to the ODPA or not, the controller must keep a written record of each personal data breach of which the controller is aware, including the facts relating to the breach, the effects, the remedial action taken and any steps taken by the controller to comply with its notification obligations (including a copy of the notice provided to the ODPA).

Notice to data subjects:

Where a controller becomes aware of a personal data breach that is likely to pose a "high risk to the significant interests of a data subject," the controller must give the data subject written notice of the breach as soon as possible.

The Breach Guidance provides a non-exhaustive of factors for controllers to take into account when determining whether a breach poses a high risk. While financial loss, reputational damage and identity fraud must be considered, the Breach Guidance also includes the risk of whether the breach might have an adverse impact of safety or well-being of the data subject (including psychological distress or humiliation). When assessing the risks, the ODPA expects all controllers to consider the nature, scope, context and purpose of the compromised personal data (including whether special category data had been compromised).

Such notice must include a description of the nature of the breach, the name and contact details of the DPO or point of contact, a description of the likely consequences of the breach, and a description of the measures taken or proposed to be taken by the controller to address the breach.

A controller is exempt from the requirement to notify a data subject where it has done either of the following:

- Established and carried out appropriate technical and organizational measures to protect personal data and, in particular, those measures have rendered personal data unintelligible to any person who is not authorized to access it (e.g., encryption)
- Taken subsequent measures to mitigate the risk, such that the high risk is no longer likely to materialize, or where the performance of the duty would involve disproportionate effort

While the Breach Guidance does not define what might constitute disproportionate effort, it clarifies that a controller must nonetheless publish a notice (without making public any personal data) or take any other step equivalent to publication in order to inform the data subjects in an equally effective manner.

Notice to controller (where a processor is engaged):

The responsibility for reporting a personal data breach to the ODPA rests with the controller. However, where a processor becomes aware of a personal data breach, the processor must give the controller notice as soon as practicable. Where notice is given orally, written notice must follow at the first available opportunity.

Other regulatory notification requirements:

Guernsey's European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance 2004 ("e-Privacy Ordinance") requires a provider of a public electronic communications service (the "service provider") to notify subscribers of a significant risk to the security of the service.

ENFORCEMENT

The DP Authority and the ODPA are responsible for administering and enforcing the DPL 2017 (Section 61(1)(a) DPL 2017).

When investigating a complaint regarding a potential breach of the DPL 2017, the DP Authority has wide powers to require information and, with appropriate warrants, powers to enter premises and search them (Schedule 7 DPL 2017). It may also conduct and/or require an audit of a controller or processor.

Before making a breach determination or an enforcement order, the ODPA may give the person concerned a written notice of the ODPA's proposals and allow the person time (up to 28 days) to make representations. However, the ODPA may dispense with this requirement if the determination or order needs to be made immediately or without notice in the interests of the data subjects or where the ODPA has reasonable grounds for suspecting that the notice may be tampered with or might seriously prejudice any other investigations etc. There is also a right to appeal the decision of the ODPA under section 84 DPL 2017.

Following a breach determination, the ODPA may take the following enforcement action:

Reprimand

The DPL 2017 does not specify the conditions upon which a reprimand may be issued. However, it will most likely take the form of a notice, and may be issued in combination with an administrative fine or a formal undertaking by the controller or processor to meet future compliance with any part of the DPL 2018.

Warning

A warning may be given where the ODPA determines that any proposed processing or other act or omission is likely to be breach the DPL.

Order

This refers to a formal notice of enforcement and can order any or all of the following:

- Bring specified processing operations into compliance with an operative provision of the DPL 2017, or take any other specified action required to comply with said provision, in a manner and within a period specified in the order
- Notify a data subject of any personal data breach
- Comply with a request made by the data subject to exercise a data subject right
- Rectify or erase personal data
- Restrict or limit the recipient's processing operations (which may include restricting or ceasing the processing operation or suspending any transfers to an unauthorized jurisdiction)
- Notify persons to whom the personal data has been disclosed of the rectification, erasure or temporary restriction on processing

Administrative Fines:

While the GDPR has the potential to attract administrative fines of up to 4% of annual worldwide turnover or €20 million (whichever is higher), the administrative fines under the DPL 2017 are generally lower (between £5 million - £10 million) and can be categorized according to various levels.

Level 1:

Administrative fines issued against a controller or processor may not exceed £5 million for breaches of section 74(1)(a) – (d) DPL 2017, comprising the following:

- Failure to make reasonable efforts to verify that person giving consent to the processing of the personal data of a child under 13 years of age in the context of the offer of information society services directly to the child is a person duly authorized to give consent to that processing under Section 10(2)(f) DPL 2017
- Failure to take reasonable steps to inform the data subject of anonymization (in breach of Section 11(1)(b) DPL 2017)
- Any breach of the general duties of controllers and processors (except section 31 DPL 2017 – duty to take reasonable steps for compliance) (breach of Part IV DPL 2017)
- Any breach of a controller's administrative duties including the requirement to designate a representative in the Bailiwick in certain cases and the requirement to register and pay fees to the ODPA (as per Part V DPL 2017)
- A breach of the security provisions contained in Part VI DPL 2017
- Failure to comply with the requirements in respect of data protection impact assessments and prior consultation (except section 46 DPL 2017 – prior consultation required for high-risk legislation) in accordance with Part VII DPL 2017
- Failure to comply with requirements to designate a DPO (where required) or ancillary duties relating to the DPO's functions in accordance with breach of VIII DPL 2017

Level 2:

Administrative fines issued against a controller or processor may not exceed £10,000,000 for breaches of section 74(1) DPL 2017, comprising the following (in addition to the Level 1 list above):

- Breach of any duty imposed on the person concerned by section 6(1) (data protection principles) including lawfulness of processing
- Breach of any duty imposed on the person concerned under Part III DPL 2017 (data subject rights)
- Failure to comply with an order by the DP Authority under section 73(2) DPL 2017 within the time specified in the order
- Transfer of personal data to a person in an unauthorized jurisdiction in breach of section 55 DPL 2017 (general prohibition of transfers of personal data outside of the Bailiwick to unauthorized jurisdictions)
- Breach of any provision of any ordinance or regulations made pursuant to the DPL 2017 which imposes a duty on a controller or processor

Level 3:

In addition to the two administrative fines described above, the DPL 2017 imposes a cap on administrative fines of up to £300,000 (unless the fine is less than 10% of the person's total annual global turnover or total global gross income in the preceding financial year).

Level 4:

An administrative fine issued against a person must not exceed 10% of the total global annual turnover or total global gross income of that person during the period of the breach in question, up to three years.

Offenses/Criminal Proceedings

In addition to the above, the DPL 2017 imposes criminal sanctions on persons who are found guilty of certain specified offenses. Such offenses include:

- Unlawful obtaining or disclosure of personal data
- Obstruction or provision of false, deceptive or misleading information

- Impersonation of a DP Authority official
- Unless an exception applies and breach of confidentiality by a designated official without the consent of the individual

Regarding the offense under the last bullet above, a designated official shall include a member of the DP Authority including the Commissioner and any DPO.

Criminal liability can attach to any director or other officer of the organization (including a body corporate, general partner of a limited partnership, foundation official). Criminal proceedings may also be instigated against an unincorporated entity in the case of a general partnership.

ELECTRONIC MARKETING

Direct marketing by electronic means to individuals and organizations is regulated by the European Communities (Implementation of Privacy) Directive (Guernsey) Ordinance 2004 ("e-Privacy Ordinance").

Following the implementation of the DPL 2017, the e-Privacy Ordinance was amended consequentially to conform outdated references to the new law and replace references to the Data Protection Commissioner with Data Protection Authority. No material amendments were made to the e-Privacy Ordinance, which is intended to sit alongside the DPL 2017.

In this regard, neither the e-Privacy Ordinance nor the DPL 2017 prohibit the use of personal data for the purposes of electronic marketing provided that individuals have the right to prevent the processing of their personal data (*ie*, a right to 'opt out') for direct marketing purposes.

As such, the e-Privacy Ordinance still reflects the e-Privacy Directive and therefore prohibits the use of automated calling systems without the consent of the recipient. Furthermore, unsolicited emails can only be sent without consent if the following conditions are met:

- The contact details have been provided in the course of a sale or negotiations for a sale
- The marketing relates to a similar product or service
- The recipient was given a simple method of refusing the use of their contact details when they were collected

The identity of the sender cannot be concealed in direct marketing communications sent electronically (which is likely to include SMS marketing).

These restrictions only apply in respect of individuals and not where corporations are sent marketing communications.

ONLINE PRIVACY

The 2011 amendments to the Privacy and Electronic Communications Regulations 2003 (PECR) by the UK in relation to cookies did not find their way into Guernsey law and there are no immediate plans for this to be done. However, certain aspects of online privacy nevertheless remain governed by the e-Privacy Ordinance (defined under the heading *Electronic Marketing* above).

As a matter of good practice, the use of cookies should be identified to web users and they should be allowed to opt out of their use if they so wish.

Traffic data held by a service provider must be erased or anonymized when it is no longer necessary for the purpose of a transmission or communication. Exceptions include if the information is being retained in order to provide a value added service to the data subject or if it is held with their consent.

Traffic data should only be processed by a service provider for (a) the management of billing or traffic, (b) customer enquiries, (c) the prevention or detection of fraud, (d) the marketing of electronic communications services, or (e) the provision of a value added service.

Location data may only be processed where the user / subscriber cannot be identified from that data or for the provision of a

value added service with consent.

Given the fundamental changes to the data protection regime since the e-Privacy Ordinance was introduced in 2004 and the ongoing negotiations in Europe in relation to the so-called e-Privacy Regulation ("Regulation"), further amendments to the e-Privacy Ordinance are, perhaps, inevitable. The States of Guernsey continues to monitor the progress of the draft Regulation in the meantime.

KEY CONTACTS

Carey Olsen (Guernsey) LLP
www.careyolsen.com

Alexandra Gill
Associate
T +44 (0)1481 741546
alexandra.gill@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

HONDURAS

Last modified 28 January 2019

LAW

Personal data protection is regulated mainly in:

National Constitution: Article 182 provides the constitutional protection of habeas data, giving individuals the right 'to access any file or record, private or public, electronic or hand written, that contains information which may produce damage to personal honour and family privacy. It is also a method to prevent the transmission or disclosure of such data, rectify inaccurate or misleading data, update data, require confidentiality and to eliminate false information. This guarantee does not affect the secrecy of journalistic sources.'

Law of the Civil Registry (Article 109, Decree 62-2004). This law refers only to public personal information that is contained in the archives of the Civil Registry.

Law for Transparency and for Access to Public Information (Article 3.5, Decree 170-2006). This law enables the access of any person to all the information contained in public entities, except that which is classified as 'Confidential.' It also extends the constitutional protection of habeas data and forbids the transmission of personal information that may cause any kind of discrimination or any moral or economic damage to people.

Rulings on the Law for Transparency and for Access to Public Information (Article 42, Accord 001-2008). Provide a definition of databases containing personal confidential information, and requires data subject consent, prior to the use of it by any third party.

In addition, the Law for the Protection of Confidential Personal Data (the "Law") is currently in discussion in the Honduran Congress. Congress has approved the first chapters of the Law. The complete approval of the Law and the date for when the Law will enter into force is expected in the first half of 2019.

DEFINITIONS

Definition of personal data

Public Personal Data under the Law of the Civil Registry is defined as: Public Data whose disclosure is not restricted in any way, and includes the following:

- Names and surnames
- ID number
- Date of birth and date of death
- Gender
- Domicile (but not address)
- Job or occupation
- Nationality
- Civil status

Definition of sensitive personal data

The Law for Transparency and for Access to Public Information defines 'Sensitive Personal Data' as: "Those personal data relating to ethnic or racial origin, physical, moral or emotional characteristics, home address, telephone number, personal electronic address, political participation and ideology, religious or philosophical beliefs, health, physical or mental status, personal and familiar heritage and any other information related to the honor, personal or family privacy, and self-image."

Other Definitions:

- Consent: Written and express authorization of the person to whom the personal data refers in order to disclose, distribute, commercialize, and/or use it in a different way as it was originally given for
- Confidential Information: Information provided by particular persons to the government which is declared confidential by any law, including sealed bids for public tenders
- Classified Information: Public information classified as that by the law, and / or by resolutions issued by governmental institutions

NATIONAL DATA PROTECTION AUTHORITY

Two entities are responsible for enforcing personal data protection:

1. National Civil Registry
   http://www.rnp.hn

2. Institute for the Access to Public Information
   http://www.iaip.gob.hn

REGISTRATION

Only Obligated Entities must inform the Institute for the Access to Public Information of their databases. Obligated Entities are:

- Government institutions
- NGO's
- Entities that receive public funds, and
- Trade unions with tax exemptions

The Institute for the Access to Public Information will maintain a list of the databases of the above-mentioned entities.

DATA PROTECTION OFFICERS

Only Obligated Entities must appoint a data protection officer.

COLLECTION & PROCESSING

Individuals, companies, and / or Obligated Entities that collect personal data may not use sensitive personal data or confidential information without the consent of the person to whom such information relates.

However, consent is not required to use or transfer personal data in the following cases:

- If the information is used for statistical or scientific needs, but only if the personal data is provided in a way that it cannot be associated with the individual to whom it relates

- If the information is transmitted between Obligated Entities, only if the data is used in furtherance of the authorised functions of those entities

- If ordered by a Court

- If the data is needed for the purpose it was provided to the individual or company to perform a service. Such third parties may not use personal information for purposes other than those for which it was transferred to them

- In other cases established by law

TRANSFER

Individuals and / or companies may not transfer, commercialize, sell, distribute or provide access to personal data contained in databases developed in the course of their job, except with the express and direct written consent of the person to whom that data refers, subject to certain exceptions.

SECURITY

The Institute for the Access to Public Information has the authority to require all Obligated Entities to take necessary security measures for the protection of the personal data they collect and / or use.

The current legislation neither clarifies nor specifically identifies the security policies or security mechanisms that Obligated Entities must comply with.

As a general statement, the Institute for the Access to Public Information has to ensure the security of all Public Information, of all information classified as confidential by public entities, of all sensitive personal data, and of all information to which the current legislation gives a secrecy status.

BREACH NOTIFICATION

Breach notification is not required.

ENFORCEMENT

The Institute for the Access to Public Information may receive complaints about abuses regarding the collection of personal or confidential data.

The Institute will impose corrective measures and establish recommendations for those persons or companies who disclose personal data, sensitive personal data or confidential data without authorization.

ELECTRONIC MARKETING

There is no law or regulation that specifically regulates electronic marketing.

ONLINE PRIVACY

There is no law or regulation that specifically regulates online privacy.

KEY CONTACTS

Bufete Gutiérrez Falla y Asociados
www.gufalaw.com/

Julio Alejandro Pohl Garcia Prieto
Associate
T +504 2238-2455
julio.pohl@gufalaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

HONG KONG

Last modified 28 January 2019

LAW

The Personal Data (Privacy) Ordinance (Cap. 486) (Ordinance) regulates the collection and handling of personal data. The Ordinance has been in force since 1996, but, in 2012/2013 was significantly amended (notably with regard to direct marketing).

DEFINITIONS

Definition of personal data

Personal data is defined in the Ordinance as any data:

- Relating directly or indirectly to a living individual
- From which it is practicable for the identity of the individual to be directly or indirectly ascertained, and
- In a form in which access to or processing of the data is practicable

Definition of sensitive personal data

There is not a separate concept of sensitive personal data in the Ordinance. However, non-binding guidance issued by the Office of the Privacy Commissioner for Personal Data (PCPD) (in the context of biometric data) has indicated that higher standards should be applied as a matter of best practice to more sensitive personal data.

NATIONAL DATA PROTECTION AUTHORITY

The Office of the Privacy Commissioner for Personal Data

12/F, Sunlight Tower
248 Queen's Road East
Wanchai
Hong Kong

T +852 2827 2827
F +852 2877 7026

http://www.pcpd.org.hk/

The PCPD is responsible for overseeing compliance with the Ordinance.

REGISTRATION

Currently, there is no requirement for organizations that control the collection and use of personal data (known as "data users") to register with the data protection authority.

However, under the Ordinance the PCPD has the power to specify certain classes of data users to whom registration and reporting obligations apply. Under the Data User Return Scheme (DURS), data users belonging to the specified classes are required to submit data returns containing prescribed information to the PCPD, which will compile them into a central register accessible by the public. However, at the time of writing, no register has been created to date. The PCPD has proposed to implement the DURS in phases, with the initial phase covering data users from the following sectors and industries:

- The public sector
- Banking, insurance and telecommunications industries, and
- Organizations with a large database of members (*eg*, customer loyalty schemes)

A public consultation for the DURS by the PCPD was concluded in September 2011. The PCPD had originally planned to implement the DURS in the second half of 2013. However, in January 2014, the PCPD indicated that it planned to put the DURS on hold until the reforms of the European Union (EU) data protection system have been finalized (as the Hong Kong model is broadly based on the same) but no exact time frame for the implementation has been announced. In light of the European Union General Data Protection Regulation 2016/679 (GDPR), which generally eliminated the data processing registration requirements under EU data protection law, it is unclear now whether the PCPD will implement the Hong Kong DURS scheme.

DATA PROTECTION OFFICERS

Currently, there is no legal requirement for data users to appoint a data protection officer in Hong Kong. However, in February 2014, the PCPD issued a best practice guide to advocate the development of a privacy management program and encourage data users to appoint or designate a responsible person to oversee the data users' compliance with the Ordinance. This role may or may not be a full-time job, and there is no specific requirement for a Hong Kong citizen or resident to hold this role. There is no specific enforcement action or penalty if a company does not appoint a data protection officer.

COLLECTION & PROCESSING

A data user may collect personal data from a data subject if:

- The personal data is collected for a lawful purpose directly related to a function or activity of the data user
- The collection is necessary for or directly related to that purpose
- The data to be collected is adequate but not excessive, and
- All practical steps have been taken to ensure that the data subject has been informed, on or before collection of the data, of the following:
    - Whether the supply of personal data by the data subject is obligatory or voluntary and, if obligatory, the consequences of not supplying the data
    - The purposes for which the data will be used
    - The persons to whom the data may be transferred
    - The data subject's right to request for access to and correction of their personal data, and
    - The name or job title, and address, of the individual to whom requests for access or correction should be sent

Separate, additional notice requirements apply to direct marketing (see below).

Data users may only collect, use and transfer personal data for purposes notified to the data subject on collection (see above), unless a limited exemption set out in the Ordinance applies. Any usage or transfer of personal data for new purposes requires the prescribed consent of the data subject.

Data users are also required to take all practicable steps to ensure the accuracy and security of the personal data; to ensure it is not kept longer than necessary for the fulfillment of the purposes for which it is to be used (including any directly related purpose); and to keep and make generally available their policies and practices in relation to personal data.

In October 2018, the PCPD published a "New Ethical Accountability framework." Under the framework, the PCPD is effectively urging businesses operating in Hong Kong to undertake privacy impact assessments – referred to as "Ethical Data Impact Assessments, which are already required to some extent under a number of other laws, such as China. the Philippines, as well as GDPR.

TRANSFER

Data users may not transfer personal data to third parties (including affiliates) unless the data subject has been informed of the following on or before his / her personal data was collected:

- That his / her personal data may be transferred
- The classes of persons to whom the data may be transferred

There are currently no restrictions on transfer of personal data outside of Hong Kong, as the cross-border transfer restrictions set out in section 33 of the Ordinance were held back and have not yet come into force. A proposal to implement them is under active consideration by the Hong Kong government, but this process has been delayed while consideration is given to recent developments in cross-border data transfers in the EU. If these restrictions come into force as currently drafted, they will have a significant impact upon outsourcing arrangements, intragroup data sharing arrangements, compliance with overseas reporting obligations and other activities that involve cross-border data transfer.

Nevertheless, non-binding best practice guidance published by the PCPD encourages compliance with the cross-border transfer restrictions in section 33 of the Ordinance, which prohibit the transfer of personal data to a place outside Hong Kong unless certain conditions are met (including a white list of jurisdictions; separate and voluntary consent obtained from the data subject; and an enforceable data transfer agreement for which the PCPD provides suggested model clauses).

SECURITY

Data users are required by the Ordinance to take all practical steps to ensure that personal data is protected against unauthorized or accidental access, processing, erasure, loss or use, having regard to factors including the nature of the personal data and the harm that could result if data breaches or leaks were to occur.

Where the data user engages a data processor to process personal data on its behalf, the data user must use contractual or other means to:

- Prevent unauthorized or accidental access, processing, erasure, or loss of use of the personal data, and
- Ensure that the data processor does not retain the personal data for longer than necessary

BREACH NOTIFICATION

Currently there is no mandatory requirement under the Ordinance for data users to notify authorities or data subjects about data breaches in Hong Kong. However, according to non-binding guidance issued by the PCPD, as a matter of best practice the PCPD encourages notification to the PCPD, and to data subjects where there would be a risk of harm by not notifying.

Recent high profile data incidents may lead regulators and politicians to consider introducing more stringent breach notification rules. The PCPD has already hinted at increased use of compliance checks and greater publication of investigation reports as part of "fair" enforcement of the law.

ENFORCEMENT

The PCPD is responsible for enforcing the Ordinance. Generally, unless a specific offense applies, if a data user is found to have contravened the data protection principles of the Ordinance, the PCPD may issue an enforcement notice requiring the data user to take steps to rectify the contravention. Failure to abide to the enforcement notice is a criminal offense, punishable by a fine of up to HK$50,000 and imprisonment for up to two years, as well as a daily penalty of HK$1,000 if the offense continues after conviction. In the case of subsequent convictions, additional and more severe penalties apply. There are also certain specific offenses under the Ordinance which are triggered directly without the intermediary step of an enforcement notice. For example:

- Breach of certain provisions relating to direct marketing is punishable by a fine of up to HK$1 million and imprisonment of up to five years, depending on the nature of the breach, and
- Disclosing personal data of a data subject obtained from a data user without the data user's consent is an offense punishable by a fine of up to HK$1 million and imprisonment of up to five years, where such disclosure is made with certain intent, or where the disclosure causes psychological harm to the data subject

Appeals from enforcement decisions of the PCPD may be made to the Administrative Appeals Board.

In addition to criminal sanctions, a data subject who suffers damage by reason of contravention of the Ordinance may also seek compensation from the data user through civil proceedings. The PCPD operates an assistance scheme for data subjects in this regard.

In light of recent high profile data incidents, the PCPD may further strengthen its enforcement against breaches of the Ordinance through more frequent compliance checks and publication of investigation reports. It is also expected that the government, consumer and finance / credit industries are likely to be in the spotlight of enforcement in 2019 in light of those recent data incidents.

ELECTRONIC MARKETING

Specific provisions of the Ordinance govern the use and sharing of personal data for the purposes of direct marketing (meaning the offering, or advertising the availability of goods, facilities or services, or the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes), when such marketing is conducted through "direct marketing means" (being the sending of information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or making telephone calls to specific persons).

The direct marketing provisions generally require data users who wish to use personal data for the data user's own direct marketing purposes to obtain prior consent from the data subject for such action and notify the data subject as follows:

- That the data user intends to use the individual's personal data for direct marketing
- That the data user may not so use the personal data unless the data subject has received the data subject's consent to the intended use
- The kind(s) of personal data to be used
- The class(es) of marketing subjects (*ie*, goods / services to be marketed) in relation to which the data is to be used, and
- The response channel through which the individual may, without charge, communicate the individual's consent to the intended use

Furthermore, if the consent was given orally, data users have the additional obligation to send a written confirmation to the data subject confirming the particulars of the consent received.

The direct marketing provisions generally require data users who wish to share personal data with a group company or a third party for their direct marketing purposes (*eg*, for joint marketing, or in connection with a sale of a marketing list) to obtain their prior written consent and to notify the data subject as follows:

- That the data user intends to provide the individual's personal data to another person for use by that person in direct

marketing

- That the data user may not so provide the data unless the data user has received the individual's written consent to the intended provision
- That the provision of the personal data is for gain (if it is to be so provided)
- The kind(s) of personal data to be provided
- The class(es) of persons to which the data is to be provided
- The class(es) of marketing subjects (*ie*, goods/services to be marketed) in relation to which the data is to be used, and
- The response channel through which the individual may, without charge, communicate the individual's consent to the intended use

When data users use personal data for the purposes of direct marketing for the first time, they must inform the subjects that they may opt out at any time, free of charge. In practice, it is common for most direct marketing email messages in Hong Kong contain unsubscribe functions, not just the first message.

Hong Kong's anti-spam framework is set out in the Unsolicited Electronic Messages Ordinance (Cap. 593), under which three types of Do-Not-Call (DNC) registers are maintained, namely the DNC for fax, short messages and pre-recorded telephone messages. Person-to-person telemarketing calls are not regulated by this framework.

In 2018, the Hong Kong government proposed that a statutory DNC register be set up allowing individuals who do not wish to receive person-to-person calls to register their phone numbers with the register, which shall be administered by the PCPD. The legislative proposal to implement the new DNC is being prepared by the Hong Kong government.

ONLINE PRIVACY

The principles as stated in the Ordinance also apply in the online environment. For example, under the Ordinance, data users have the obligation to inform data subjects of the purposes for collecting their personal data, even if personal data is collected through the Internet. If a website uses cookies to collect personal data from its visitors, this should be made known to them. Data users should also inform the visitors whether and how non-acceptance of the cookies will affect the functionality of the website.

KEY CONTACTS

Scott Thiel
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +852 2103 0519
scott.thiel@dlapiper.com

Carolyn Bigg
Of Counsel
T +852 2103 0576
carolyn.bigg@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

HUNGARY

Last modified 10 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Hungarian Parliament implemented the GDPR in two steps. Firstly, it adopted an amendment to the existing Act on Information (Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information) basically with two major issues:

- appointment of the Hungarian DPA, and
- a provision for the DPA to give warning instead of imposing fines for first time infringement of data protection rules

The new law is effective as of June 30, 2018.

The second amendment of the Act on Information fully adopted the GDPR and implemented the Directive for the police and criminal justice sector [Directive (EU) 2016/680]. With respect to the GDPR the amendment deregulates the Act on Information and provides institutional and procedural framework for the application of the substantive law laid down in the GDPR. The second amendment is effective as of July 26, 2018.

As a third step of harmonizing Hungarian data protection laws to the new European legislation, the amendment to the sectorial laws can be expected in 2019.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Hungarian Supervisory Authority is the Hungarian National Authority for Data Protection and Freedom of Information (in Hungarian: *Nemzeti Adatvédelmi és Információszabadság Hatóság*).

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or

processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and

organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to

requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for

ensuring the security of the processing.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg,* an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (*eg,* an email address is likely to be 'personal data' for the purposes of the Act).

Also, pursuant to Act No. XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities, unless otherwise provided by specific other legislation, advertisements may be conveyed to natural persons by way of

direct contact (hereinafter referred to as 'direct marketing'), such as through electronic mail or equivalent individual communications only upon the express prior consent of the person to whom the advertisement is addressed. The request for the consent may not contain any advertisement, other than the name and description of the company.

The statement of consent may be made in any way or form, on condition that it contains the name of the person providing it, and – if the advertisement to which the consent pertains may be disseminated only to persons of a specific age – his place and date of birth, furthermore, any other personal data authorized for processing by the person providing the statement, including an indication that it was given freely and in possession of the necessary legal information.

The statement of consent may be withdrawn freely any time, free of charge and without any explanation. In this case all personal data of the person who has provided the statement must be promptly erased from the records and all advertisements must be stopped.

Pursuant to Act No. C of 2003 on Electronic Communications ('EC Act'), applying automated calling system free of any human intervention, or any other automated device for initiating communication in respect of a subscriber for the purposes of direct marketing, providing information, public-opinion polling and market research shall be subject to the prior consent of the subscriber.

ONLINE PRIVACY

The EC Act deals with the collection of location and traffic data by public electronic communications services providers ('CSPs') and use of cookies (and similar technologies).

Traffic Data

With certain special exceptions set out in the EC Act (*eg*, invoicing, collecting subscriber fees, law enforcement, national security and defense), traffic data relating to subscribers and users processed and stored by CSPs while providing such services must be erased or made anonymous when it is no longer needed.

CSPs may use certain traffic data as referred to in the EC Act for the provision of value added services or for marketing purposes subject to the subscriber's or user's prior consent, to the extent necessary for the provision of such services or for marketing purposes. CSPs shall provide the possibility for users or subscribers to withdraw their consent at any time.

Location Data

CSPs shall be authorized to process location data only upon the prior consent of the subscribers or users to whom the data are related, and only to the extent and for the duration as it is necessary for the provision of value added services.

Users and subscribers shall have the right to withdraw their consent at any time.

CSPs shall be required to comply with any request for location information in connection with specific subscribers or users, if made by the investigating authority, the public prosecutor, the court or the national security service pursuant to the authorization conferred in specific other legislation, to the extent required to discharge their respective duties.

Cookie Compliance

Pursuant to the EC Act, on the electronic communication terminal equipment of a subscriber or user, information may be stored, or accessed, only upon the user's or subscriber's prior consent granted in possession of clear and comprehensive information, which information inter alia includes the purpose of processing.

The competent Hungarian Authorities have not issued any guidance in respect of the interpretation of 'consent' and how this consent should be obtained in practice. General practice is that consent can be obtained via browser settings, however, as mentioned so far this has not been confirmed by the opinion or the guidance of the Authorities yet.

KEY CONTACTS

Csaba Vari
Senior Associate
csaba.vari@dlapiper.com

Zoltan Kozma
Counsel
T +3615101154
zoltan.kozma@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ICELAND

Last modified 17 October 2018

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Act No. 90/2018 on Data Protection and the Processing of Personal Data (the 'DPA') implements the GDPR in Iceland. The law contains derogations and exemptions from the position under the GDPR in certain permitted areas.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The DPA defines a public authority or body in accordance with Article 1 of the Administrative Procedures Act no. 37/1993. The term public authority refers to all parties, institutions, committees, etc. which are governed by state and local government.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Data Protection Authority (Icelandic: '*Persónuvernd*') is the supervisory authority in Iceland for the purposes of Article 51 of the GDPR.

Contact details:
Persónuvernd – The Icelandic Data Protection Authority
Rauðarárstígur 10, 105 Reykjavík, Iceland.
Tel. +354 510-9600
e-mail: postur@personuvernd.is
www.personuvernd.is

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or

processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

According to Article 31 of the DPA, controllers need to consult with and obtain prior authorization from the supervisory authority in relation to processing by a controller for the performance of a task carried out in the public interest, including processing in relation to social protection and public health. The GDPR generally implies certain withdrawal from the previous policy that processing of personal data may be based on licenses, but this Article in the DPA is an exception.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

Iceland did not extend the requirement to appoint a Data Protection Officer, cv. Article 37(4) of the GDPR.

The DPA defines a public authority or body in accordance with Article 1 of the Administrative Procedures Act no. 37/1993. The term public authority refers to all parties, institutions, committees, etc. which are governed by state and local government. According to the bill to the DPA, it is regarded desirable that companies entrusted with certain projects

for the public interest designate a Data Protection Officer with regard to those projects.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally

incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);

- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Criminal convictions and offences data (Article 10)

According to Article 12 of the DPA, processing of personal data relating to criminal convictions and offences is subject to certain conditions and the processing must be based on one of the legal basis in Article 9 of the DPA, cf. Article 6(1) of the GDPR.

According to Article 12(1) of the DPA, authorities may not process data relating to criminal convictions and offences unless it is necessary for the purpose of their statutory tasks.

According to Article 12(2) of the DPA, the data cannot be disclosed unless:

- the data subject has explicitly given its consent for the disclosure
- disclosure is necessary for the legitimate interests of the public or private sector which obviously outweigh the interests of the confidentiality of the data, including the interests of the data subject
- the disclosure is necessary for the legitimate tasks of the relevant authority or for the authority's decision or disclosure is necessary for public-sector projects that have been legally assigned to private parties

Private entities cannot process information on criminal convictions and offences unless the data subject has given its explicit consent or the processing is necessary for legitimate interests which obviously outweigh the interest of the data subject.

Children's consent to information society services (Article 8)

Article 8(1) of the GDPR stipulates that a child may only provide their own consent to processing in respect of information society (primarily, online) services, where that child is over 16 years of age, unless member state law applies a lower age. The DPA reduces the age of consent for these purposes to 13 years for Iceland, cf. Article 10(5).

Data subject's rights

The data subject has the right to be informed about the processing of his personal data, however, Article 17 of the DPA implements certain restrictions from these rights.

According to Article 17(3) of the DPA, Articles 13(1)-(3), 14(1)-(4) and 15 of the GDPR regarding the data subjects' rights do not apply if the interests of individuals linked to the personal data, including the interests of the data subject itself, outweigh the interests of the data subject.

The rights granted to the data subject in Articles 13 – 15 of the GDPR can be restricted with a legislative measure if such a limitation of fundamental rights and freedoms constitutes necessary and proportionate measure in a democratic society to safeguard:

- national security
- national defense
- public security
- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security
- other important objectives of general public interest, in particular those of economic or financial interest including monetary, budgetary and taxation matters, public health and social security
- the protection of the data subject, the vital interests of the public or the fundamental rights of others
- the enforcement of civil law claims
- legal obligation of professional secrecy

The right to restrict the data subjects right also applies to personal data in working documents used in preparation for the controllers' decisions if it has not been distributed to others, to the extent necessary to ensure the preparation of the proceedings.

Information regarding cases that are being processed by authorities may be exempted from access according to Article 15(1) of the GDPR to the same extent as applies according to the Information Act no. 140/2012 and the Administrative Procedures Act no. 37/1993.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data

subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Regarding the security of the processing and notification of a personal data breach, Articles 32 and 33 of the GDPR are implemented in the DPA without alterations in Article 27.

The Icelandic Data Protection Authority has issued guidelines for notifications of security breaches which are based on the instructions of the Article 29 Working Party on security breaches and has provided a form for notification purposes.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf

(Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Non-compliance with the instructions of the Data Protection Authority regarding a) temporary or definitive limitation including a ban on processing, b) rectification or erasure of personal data or restriction of processing and the notification of such actions to recipients to whom the personal data have been disclosed, or c) suspension of data flows to a recipient in a third country or to an international organization, can lead to daily fines until necessary improvements have been made. Fines can amount up to ISK 200,000 (approximately 1,600 euros) for each day that passes without the Data Protection Authority's instructions being observed.

Breaches of the DPA can lead to fines from ISK 100,000 (approximately 800 euros) to 1,2 billion ISK (approximately 9,600 euros) (in relation to Article 83(4) of the GDPR) and ISK 100,000 to ISK 2,4 billion (approximately 19,280 euros) (in relation to Articles 83(5)-83(6) of the GDPR), cf. Article 46 of the DPA.

Major breaches can also lead to imprisonment up to 3 years and breach of confidentiality of a data protection officer can lead to fines or imprisonment up to 1 year and in severe cases, up to 3 years, cf. Article 48 of the DPA.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Based on the Electronic Communications Act No 81/2003 the use of electronic communications systems, including for email and other direct marketing, is only allowed if a subscriber has given prior consent.

If the email address has been obtained in the context of the sale of a good or service, the controller may use it for direct marketing of the controller's own goods or services to customers who have not objected to receiving email marketing from the controller, provided the customers are given the opportunity, free of charge, to object to such use of their email address when it is collected and each time a message is sent.

Further, all marketing emails must include the name and address of the party responsible for the marketing.

ONLINE PRIVACY

There are no provisions in Icelandic legislation that specifically deal with the use of cookies or location data. However, location data and IP addresses are considered personal data under the Data Protection Act.

If the use of cookies leads to the use of IP addresses or other personal data, the processing of such data must comply with the Data Protection Act. The processing is therefore not permissible unless one of the listed conditions is met, in most instances the data subject must consent to the processing of such data.

KEY CONTACTS

LOGOS Legal Services
www.logoslegalservices.com

Hjördís Halldórsdóttir
Partner
T +354 5 400 300
hjordis@logos.is

Áslaug Björgvinsdóttir
Partner
T +354 5 400 300
aslaug@logos.is

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

INDIA

Last modified 28 January 2019

LAW

On August 24, 2017, a Constitutional Bench of nine judges of the Supreme Court of India in *Justice K.S.Puttaswamy (Retd.)* v. *Union of India* [Writ Petition No. 494/ 2012] upheld that privacy is a fundamental right, which is entrenched in Article 21 [Right to Life & Liberty] of the Constitution. This led to the formulation of a comprehensive Personal Data Protection Bill 2018.[1] However, presently the Information Technology Act, 2000 (the Act) contains specific provisions intended to protect electronic data (including non-electronic records or information that have been, are currently or are intended to be processed electronically).

India's IT Ministry adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules). The Privacy Rules, which took effect in 2011, require corporate entities collecting, processing and storing personal information, including sensitive personal information, to comply with certain procedures. It distinguishes both 'personal information' and 'sensitive personal information', as defined below.

In August 2011, India's Ministry of Communications and Information issued a 'Press Note' Technology (Clarification on the Privacy Rules), which provided that any Indian outsourcing service provider/organization providing services relating to the collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligation with any legal entity located within or outside India is not subject to collection and disclosure of information requirements, including the consent requirements discussed below, provided that they do not have direct contact with the data subjects (providers of information) when providing their services.

[1] This Bill has not been introduced in the Parliament, but proposes a legal framework to protect the autonomy of individuals in relation to their personal data, to specify where the flow and usage of personal data is appropriate, to create a relationship of trust between persons and entities processing their personal data, to specify the rights of individuals whose personal data are processed, to create a framework for implementing organizational and technical measures in processing personal data, to lay down norms for cross-border transfers of personal data, to ensure the accountability of entities processing personal data, to provide remedies for unauthorized and harmful processing, and to establish a Data Protection Authority for overseeing processing activities.

DEFINITIONS

Definition of personal data

The Privacy Rules define the term personal information as any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, is capable of identifying such person.

Definition of sensitive personal data

The Privacy Rules define 'sensitive personal data or information' to include the following information relating to:

- Passwords
- Financial information eg, bank account/credit or debit card or other payment instrument details
- Physical, physiological and mental health conditions
- Sexual orientation
- Medical records and history
- Biometric information
- Any detail relating to the above clauses as provided to a corporate entity for providing services
- Any of the information received under the above clauses for storing or processing under lawful contract or otherwise

Biometrics means the technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements and DNA for authentication purposes.

However, any information that is freely available in the public domain is exempt from the above definition.

NATIONAL DATA PROTECTION AUTHORITY

No such authority exists.

REGISTRATION

No requirements.

DATA PROTECTION OFFICERS

Every corporate entity collecting sensitive personal information must appoint a Grievance Officer to address complaints relating to the processing of such information, and to respond to data subject access and correction requests in an expeditious manner but within one month from the date of receipt of the request or grievance.

There is no specific requirement that the data protection officer must be a citizen of or resident of India, nor are there any specific enforcement actions or penalties associated with not appointing a data protection officer correctly. However, appointment of a data protection officer is part of the statutory due diligence process and it is thus imperative that such an officer should be appointed.

COLLECTION & PROCESSING

Under the Act, if a corporate entity that possesses, manages or handles any sensitive personal information in a computer resource that it owns, controls or operates, is negligent in implementing and maintaining compliance with the Privacy Rules, and its negligence causes wrongful loss or wrongful gain to any person, the corporate entity shall be liable for damages to the person(s) affected.

The Privacy Rules state that any corporate entity or any person acting on its behalf that collects sensitive personal information must obtain written consent (through letter, email or fax) from the providers of that information. However, the August 2011 Press Note issued by the IT Ministry clarifies that consent may be given by any mode of electronic communication.

The Privacy Rules also mandate that any corporate entity (or any person, who on behalf of such entity) that collects, receives, possess, stores, deals or handles information shall provide a privacy policy that discloses its practices regarding the handling and

disclosure of personal information, including sensitive personal information, and ensure that the policy is available for view, including on the website of the corporate entity (or the person acting on its behalf). Specifically, the corporate entity must ensure that the person to whom the information relates is notified of the following at the time of collection of sensitive personal information or other personal information:

- The fact that the information is being collected
- The purpose for which the information is being collected
- The intended recipients of the information
- The name and address of the agency that is collecting the information and the agency that will retain the information

Further, sensitive personal information may only be collected for a lawful purpose connected with a function or purpose of the corporate entity and only if such collection is considered necessary for that purpose. The corporate entity must also ensure that it does not retain the sensitive personal information for longer than it is required and should also ensure that the sensitive personal information is being used for the purpose for which it was collected.

A corporate entity or any person acting on its behalf is obligated to enable the providers of information to review the information they had so provided and also to ensure that any personal information or sensitive personal information that is found to be inaccurate or deficient is corrected upon request. Further, the provider of information has to be provided a right to opt out (*ie*, he/she will be able to withdraw his or her consent) even after consent has been provided. However, the corporate entity will not be held responsible for the authenticity of the personal information or sensitive personal information given by the provider of information to such corporate entity or any other person acting on its behalf.

TRANSFER

The data collector must obtain the consent of the provider of the information for any transfer of sensitive personal information to any other corporate entity or person in India, or to any other country that ensures the same level of data protection as provided for under the Privacy Rules. However, consent is not necessary for the transfer if it is required for the performance of a lawful contract between the corporate entity (or any person acting on its behalf) and the provider of information or as otherwise specified in the Act.

A corporate entity may not transfer any sensitive personal information to another person or entity that does not maintain the same level of data protection as required by the Act.

The contract regulating the data transfer should contain adequate indemnity provisions for a third party breach, should clearly specify the end purposes of the data processing (including who has access to such data) and should specify a mode of transfer that is adequately secured and safe.

Further, under the Act, it is an offense for any person who has pursuant to a contract gained access to any material containing personal information to disclose that information without the consent of the person concerned, and with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain.

Thus, contracts should also specifically include provisions:

- Entitling the data collector to distinguish between 'personal information' and 'sensitive personal information' that it wishes to collect/process, and
- Representing that the consent of the person(s) concerned has been obtained for collection and disclosure of personal information or sensitive personal information, and outlining the liability of the third party

Data Localization

India's central bank, the Reserve Bank of India (RBI) has made it mandatory from October 15, 2018, for all payment system providers and their service providers, intermediaries, third party vendors and other entities in the payment ecosystem to ensure that all data relating to payment systems operated by them are stored in a system only in India. Interestingly, by virtue of this regulation, RBI is seeking storage of all payment system data, which includes the entire payment processing cycle from request to final payout.

SECURITY

A corporate entity possessing, dealing or handling any sensitive personal information in a computer resource which it owns, controls or operates is required to implement and maintain reasonable security practices and procedures to secure the sensitive personal information. The reasonable security practices and procedures may be specified in an agreement between the parties.

Further, the Privacy Rules provide that in the absence of such agreement 'reasonable security practices and procedures' to be adopted by any corporate entity to secure sensitive personal information are procedures that comply with the IS/ISO/IEC 27001 standard or with the codes of best practices for data protection as approved by the federal government. Presently, no such codes of best practices have been approved by the federal government.

BREACH NOTIFICATION

The government of India has established and authorized the Indian Computer Emergency Response Team ("Cert-In") to collect, analyze and disseminate information on cyber incidents, provide forecasts and alerts of cybersecurity incidents, provide emergency measures for handling cybersecurity incidents and coordinate cyber incident response activities.

The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("Cert-In Rules") impose mandatory notification requirements on service providers, intermediaries, data centers and corporate entities, upon the occurrence of certain cybersecurity incidents.

Cybersecurity incidents have been defined to mean any real or suspected adverse events, in relation to cybersecurity, that violate any explicitly or implicitly applicable security policy, resulting in:

- Unauthorized access, denial or disruption of service
- Unauthorized use of a computer resource for processing or storage of information
- Changes to data or information without authorization

The occurrence of the following types of cybersecurity incidents trigger the notification requirements under the Cert-In Rules:

- Targeted scanning or probing of critical networks or systems
- Compromise of critical information or system
- Unauthorized access of IT systems or data
- Defacement of websites or intrusion into websites and unauthorized changes, such as inserting malicious codes or links to external websites
- Malicious code attacks such as spreading viruses, worms, Trojans, Botnets or Spyware
- Attacks on servers such as Database, Mail and DNS or network devices such as Routers
- Identity theft, Spoofing and phishing attacks
- Denial of service (DoS) and Distributed Denial of service (DDoS) attacks
- Attacks on critical infrastructure, SCADA systems and wireless networks

- Attacks on applications such as e-governance and e-commerce

Upon the occurrence of any of the aforementioned events, companies are required to notify the Cert-In within reasonable time, so as to leave scope for appropriate action by the authorities. However, it is important to follow breach notice obligations, which would depend upon the "place of occurrence of such breaches" and whether or not Indian customers have been targeted. The format and procedure for reporting of cybersecurity incidents have been provided by Cert-In on its official website.

ENFORCEMENT

Civil penalties of up to €694,450 for failure to protect data including sensitive personal information may be imposed by an Adjudicating Officer; damages in a civil suit may exceed this amount.

Criminal penalties of up to three years of imprisonment or a fine up to €6,950, or both for unlawful disclosure of information.

ELECTRONIC MARKETING

The Act does not refer to electronic marketing directly. Dishonestly receiving data, computer database or software is an offense. However, in a related development, the Food Safety and Standards Authority of India (FSSAI) has made it mandatory for E-commerce FBOs (Food Business Operators) to obtain a license from the Central Licensing Authority. E-commerce FBO means any Food Business Operator carrying out any of the activities in section 3(n) of Food Safety & Standards Act, 2006, through the medium of e-commerce. Interestingly, section 3(n) covers the entire food chain as it defines "food business" as any undertaking, whether for-profit or not, and whether public or private, carrying out any of the activities related to any stage of manufacture, processing, packaging, storage, transportation, distribution of food, import and includes food services, catering services, sale of food or food ingredients. Similarly, another set of legal Rules being referred as "E-commerce & the Legal Metrology (Packaged Commodities) Amendment Rules, 2017," effective from January 1, 2018, has made it mandatory for an e-commerce entity to ensure mandatory declarations about the commodity displayed on the digital and electronic network used for e-commerce transactions.

The Privacy Rules also provide the right to "opt out" of email marketing, and the company's privacy policy must address marketing and information collection practices. Further, the National Do Not Call (NDNC) Registry is effectively implemented by the Telecom Regulatory Authority of India (TRAI). TRAI has also established the Telecom Commercial Communication Customer Preference Portal, *ie*, a national data base containing a list of the telephone numbers of all subscribers who have registered their preferences regarding the receipt of commercial communications. Telemarketing companies may lose their license for repeated violation of DNC norms.

ONLINE PRIVACY

There is no regulation of cookies, behavioral advertising or location data. However, it is advisable to obtain user consent, such as through appropriate disclaimers.

However, the IT Act contains both civil and a criminal offenses for a variety of computer crimes:

- Any person who introduces or causes to be introduced any computer contaminant into any computer, computer system or computer network may be fined up to €694,450 (by an Adjudicating Officer); damages in a civil suit may exceed this amount. Under the IT Act, 'computer contaminant' is defined as any set of computer instructions that are designed:
    - To modify, destroy, record, or transmit data or programs residing within a computer, computer system or computer network, or
    - By any means to usurp the normal operation of the computer, computer system or computer network
- Any person, who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, is subject to a prison term of up to three years and a fine up to €1,390.

KEY CONTACTS

Vakul Corporate Advisory Pvt. Ltd

Vakul Sharma
Managing Partner
T +91 11 47025460
vakul@vakulcorp.com

Seema Sharma
Senior Partner
T +91 11 47025460
seema@vakulcorp.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

INDONESIA

Last modified 28 January 2019

LAW

Specific Regulations

In Indonesia, as of the date of this publication there is no general law on data protection. However, there are certain regulations concerning the use of electronic data. The primary sources of the management of electronic information and transactions are Law No. 11 of 2008 regarding Electronic Information and Transactions (EIT Law) as amended by Law No. 19 of 2016 regarding the Amendment of EIT Law (EIT Law Amendment), Government Regulation No. 82 of 2012 regarding Provisions of Electronic systems and Transactions (Reg. 82) and its implementing regulation, Minister of Communications & Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System (MOCI Regulation).

However, a new draft Bill on the Protection of Private Personal Data (the Bill) is being discussed and as of this date it has not been issued. Although the exact date remains uncertain and the Bill is still to be considered by the House of Representatives, if passed, this will become Indonesia's first comprehensive law to specifically deal with the issue of data privacy.

In addition to the provisions under EIT Law, Reg. 82 and MOCI Regulation, there are also a series of regulations which also cover certain provisions which may relate to data protection, such as:

Telecommunications Sector

Article 40 of Law No. 36 of 1999 regarding Telecommunications ('Telecommunications Law') provides that any person is prohibited from any kind of tapping of information transmitted through any kind of telecommunications network. Article 42 of the Telecommunications Law stipulates that any telecommunications services operator has to keep confidential any information transmitted or received by a telecommunications service subscriber through telecommunications networks or telecommunications services provided by the relevant operator.

Public Information Sector

Article 6 of Law No. 14 of 2008 regarding Disclosure of Public Information provides that information relating to personal rights may not be disclosed by public bodies. Article 17 of the relevant law, together with other laws, prohibits the disclosure of private information of any person, particularly that which concerns family history; medical and psychological history; financial information (including assets, earnings and bank records) and evaluation records concerning a person's capability, recommendation, intellectual, formal, or informal education records.

Banking and Capital Markets Sectors

Data privacy in this sector is regulated under Law 7 of 1992 as amended by Law 10 of 1998 on Banking ('Banking Law') and Law 8 of 1995 on Capital Markets (Capital Markets Law) respectively. The regulations apply to both individuals and corporate data.

Bank Indonesia's Regulation No. 9/15/PBI/2007 on the Implementation of Risk Management in the Utilization of Information Technology by the Bank stipulates that the bank's customer data transfer (by way of establishing a data center or data processing outside the Indonesia territory) necessitates prior approval being obtained from Bank Indonesia.

DEFINITIONS

Definition of personal data

Reg. 82 and MOCI Regulation defines Personal Data as: data of an individual, which is stored, maintained and which correctness is preserved and of which its confidentiality is protected (including under the EIT Law and Reg 82).

Definition of sensitive personal data

Currently, there is no specific definition on sensitive personal data under the prevailing laws and regulations.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority for data privacy in general in Indonesia.

For example, the Indonesian Financial Services Authority ('FSA') has the authority to act as the regulator of data privacy in the capital markets sector (since December 31, 2012) and with regard to banks' customer data privacy issues (since December 31, 2013).

However, please note that article 65 of Reg. 82 provides that a business enactor who operates electronic transactions may be certified by a Competence Certification Body (*Lembaga Sertifikasi Keandalan*) which may be a domestic Indonesian (but currently no such domestic bodies exist) or foreign competence certification body.

REGISTRATION

Minister of Communication and Informatics Regulation No. 36 of 2014 regarding Procedures of Electronic System Provider Registration (MOCI Reg 36) differentiates electronic system providers into electronic system provider for public services and electronic system provider for non-public services. An electronic system provider for public services must conduct registration, while an electronic system provider for non-public services may conduct registration, which suggests registration is not mandatory for an electronic system provider for non-public services).

MOCI Reg 36 specifically states that electronic system providers for public services are legal entities related with the government for example state institutions, government agencies, corporations in the form of state-owned enterprises, regional government-owned enterprise, or other legal entities in relation with state's mission.

Electronic system providers for non-public services are not specifically defined under MOCI Reg 36, but in general other legal entities that are not related with government, such as private corporations, can be classified as electronic system providers for non-public services.

However, the regulators interpret 'public service' in regards to electronic system provider pursuant to Government Regulation No. 96 of 2012 regarding Implementation of Law No. 25 of 2009 regarding Public Service (GR No. 96).

GR No. 96 defines Public Service as an activity or chain of activities in terms of fulfilling the service needs in accordance with the law and regulation for every citizen and individual on goods, services, and / or administrative services that are provided by the public service operator. GR No. 96 further defines Public Service Operator as every state operator institution, corporation, independent institution that are formed based on laws for public service activity, and other legal entities that are formed only for the public service activity. Law No. 25 of 2009 regarding Public Services (Law No. 25). Article 5 (1) of Law No. 25 provides that the scope of public services includes public goods and services as well as administrative services. Article 5(2) of Law No. 25 further provides that this includes education, teaching, work and business, housing, communication and information, environment, health, social security, energy, banking, transportation, natural resources, tourism and other strategic sectors.

In relation to the above, an electronic system provider for non-public services falls under the corporation (non-government

related legal entity), providing service for every citizen / individual. Therefore, an electronic system provider for non-public services is also considered as public services pursuant to GR No. 96.

Consequently, all electronic system providers, whether for public services or non-public services, must conduct registration.

Article 4 of Minister of Communications and Informatics Regulation No. 4 of 2016 regarding Management System of Information Protection (MOCI Reg. No. 4/2016) provides that there are three categories of electronic systems: (i) strategic electronic system, which is an electronic system that causes serious impact to the public interest, public services, state governance stability, or state defense and security; (ii) high electronic system, which is an electronic system that causes limited impact to the interest of certain sector and / or territory; and (iii) low electronic system, which is any other electronic system aside from strategic and high electronic systems.

Article 10 of MOCI Reg. No. 4/2016 provides that strategic and high electronic system providers (for public services) must obtain a Certificate of Management System of Information Protection, while low electronic system providers (for public services) may obtain Certificate of Management System of Information Protection.

DATA PROTECTION OFFICERS

There is no requirement in Indonesia for organizations to appoint a data protection officer.

COLLECTION & PROCESSING

EIT Law, Reg. 82 and the MOCI Regulation specifically regulates the obligation to obtain "consent" from the owner of the personal data in the case of data collection, use and processing. Article 7(1) of MOCI Regulation regulates that in obtaining and collecting Personal Data the electronic system provider must also be limited to the relevant and suitable information in accordance to its purpose and must be conducted accurately. Article 12(1) of MOCI Regulation also regulates that Personal Data can only be processed and analyzed in accordance with the needs of the electronic system provider that have been stated clearly at the time the Personal Data is obtained and collected.

Reg. 82 provide the specific provisions on the obligation for Electronic System Providers to public services to set up a data center and disaster recovery center in Indonesia, namely:

- Before an Electronic System for public services is implemented, the provider of an Electronic System must register with the Minister of Communication and Information and Technology (MOCI).
- In the provision of an Electronic System, the provider should ensure secrecy, totality and the availability of the Personal Data it manages. The provider should also ensure that the collection, the consumption and usage of Personal Data is based on the consent of the Personal Data owner, except if regulated otherwise. (Article 15(1)(b) of Reg. 82). The provider should ensure that the usage or disclosure of data is done based on consent and is in line with the objectives as disclosed to the relevant owner at the time of obtaining the data. (Article 15(1)(c) of Reg. 82).
- The provider of the Electronic System is also obliged to provide audit track records of the Electronic System.

TRANSFER

Article 22(2) of Reg. 82 regulates the transfer of data, which provides in any case that in the implementation of an Electronic System or Electronic Document aimed to transfer Electronic Information or Electronic Document, the Electronic Information or Electronic Document must be unique and (the provider shall) explain the control and possession of the Electronic Information or Electronic Document.

Article 21(1) of MOCI Regulation states that displaying, announcing, transferring, broadcasting, or opening Personal Data access in the Electronic System can only be conducted:

- By Consent (being defined as a written agreement either manually or electronically being given by the owner of Personal Data after obtaining a full explanation regarding the process for acquiring, collecting, processing, analyzing, storing, displaying, announcing, disseminating and sending, including the confidentiality or non-confidentiality of the Personal Data), except as otherwise stipulated by laws and regulations, and

- After its accuracy and compatibility with the purpose of obtaining and collecting such Personal Data is verified

Article 22(1) of the MOCI Regulation states that transferring Personal Data that is managed by an electronic system operator at the government and regional government institution including the public or private sector domiciled in the territory of Indonesia to [parties] outside the territory of Indonesia must:

- Coordinate with the MOCI or the official or institution being authorized for such purpose, and
- Implement the laws and regulations regarding the transboundary exchange of Personal Data

The implementation of the coordination as stipulated in Article 22(1)(a) of MOCI Regulation are:

- To report the implementation plan of Personal Data transfer, at least containing the clear name, designated country, recipient subject name, implementation date, and reason / purpose of the transfer
- To request for advocacy, if needed
- To report the activities implementation result

SECURITY

The obligations of Electronic System Providers are regulated under Reg. 82 and MOCI Regulation, which include:

- Guarantee the confidentiality of the source code of the software
- Ensure agreements on minimum service level and information security towards the information technology services being used as well as security and facility of internal communication security it implements
- Protect and ensure the privacy and personal data protection of users
- Ensure the appropriate lawful use and disclosure of the personal data
- Provide data center and disaster recovery center (for Electronic System Providers for public services)
- Provide the audit records on all Provision of Electronic Systems activities
- Provide information in the Electronic System based on legitimate request from investigators for certain crimes
- Provide options to the Personal Data Owner regarding the Personal Data that is processed so that [the Personal Data] can or cannot be used or displayed by a third party based on the Consent as long as it is related with the purpose of obtaining and collecting the Personal Data
- Provide access or opportunity to the Personal Data Owner to change or renew their Personal Data without disturbing the system management of the Personal Data, except as otherwise regulated by laws and regulations
- Delete the Personal Data if: (i) it has reached the maximum period of storing the Personal Data (at the shortest five years or based on the applicable regulations / specific sectoral regulations); or (ii) by request from the Personal Data Owner, except as otherwise regulated by laws and regulations, and
- Provide a contact person that is easy to be contacted by the Personal Data Owner in relation to their Personal Data

In the telecommunication sector, Article 19 of Minister of Communication and Informatics Regulation No. 26/PER/M.KOMINFO/05/2007 regarding the Security and Utilization of Internet Protocol based Telecommunications Network (as amended) (MR 26/2007) also provides that the telecommunication service provider is responsible for data storage due to its obligation to record its log file for at least three months.

BREACH NOTIFICATION

Article 15(2) of Reg. 82 provides that the provider of an Electronic System must provide written notification to the owner of personal data upon its failure to protect the personal data.

Article 20(3) of Reg. 82 states that the provider of an Electronic System must make the utmost effort to protect personal data and to immediately report any failure or serious system interference or disturbance to a law enforcement official or the Supervising and Regulatory Authority of the relevant sector.

Article 28(c) of the MOCI Regulation provides that a written notice to the Personal Data Owner is required if there is a failure in protecting the secrecy of the Personal Data in the Electronic System. The provisions of the notice are as follows:

- Must provide the reason or cause of the occurrence of the failure in protecting the secrecy of Personal Data. This can be provided electronically, if the Personal Data Owner has given Consent for it at the time of obtaining and collecting their Personal Data
- Must ensure that the notice has been received by the Personal Data Owner if the failure contains potential loss to the relevant Personal Data Owner, and
- The written notice is sent to the Personal Data Owner no later than 14 days after the failure is discovered

ENFORCEMENT

In Indonesia, the sanctions for breaches of data privacy are found under the relevant legislation and are essentially fines. Imprisonment may be imposed in severe instances, such as in the event of intentional infringement.

The EIT Law and EIT Law Amendment provides criminal penalties ranging from:

- Rp600 million fine to Rp800 million and six to eight years imprisonment for unlawful access
- Rp800 million fine and 10 years imprisonment for interception or wiretapping of a transmission
- Rp2 billion to Rp5 billion and 8 to 10 years imprisonment for alteration, addition, reduction, transmission, tampering, deletion, moving or hiding Electronic Information or Electronic Records

Failure to comply with Reg. 82 is subject to administrative sanctions (which do not eliminate any civil and criminal liability). These administration sanctions are in the forms of:

- Written warning
- Administrative fines
- Temporary dismissal
- Expulsion from the list of registrations (as required under the regulation)

Failure to comply with MOCI Regulations is subject to administrative sanctions in the form of:

- Verbal warning
- Written warning
- Temporary dismissal of activities
- An announcement in the online website

Banking Law

Under Article 47 of the Banking Law, any commissioner, director or employee of a bank or its affiliates who intentionally provides information which has to be kept secret may be sentenced to imprisonment for not less than 2 years but not more than 4 years, and fined at least Rp4 billion but not more than Rp8 billion.

Capital Markets Law

Under Capital Markets Law, the Financial Services Authority (Previously BAPEPAM LK) is empowered to impose the following administrative sanctions for breaches of the provisions dealing with data protection). The sanctions include:

- A written reminder
- A fine
- Limitations on business
- Suspension of business
- Revocation of business license
- Cancellation of approval
- Cancellation of registration

ELECTRONIC MARKETING

EIT Law and Reg. 82 do not specifically address electronic marketing. Article 25 of the EIT Law provides that an Internet website,

among other things, is acknowledged and protected as an Intellectual Property (IP) and consequently, should fall under the ambit of the relevant IP laws, which may in certain cases fall under the Indonesian Copyright Law.

ONLINE PRIVACY

There are currently no laws and regulations concerning cookies and location data. However, if the data collected by cookies or location data is obtained by the unlawful access of another party's electronic information, this is subject to six to eight years imprisonment and / or a fine of Rp600 million to Rp800 million.

KEY CONTACTS

Ivan Almaida Baely & Firmansyah
www.iab-net.com

Erwin Purba
Partner
T +62 21 5790 5090
erwin.purba@iab-net.com

Robert Hasan
Associate
T +62 21 5790 5090
robert.hasan@iab-net.com

Fariz Ghassen
Associate
T +62 21 5790 5090
fariz.ghassen@iab-net.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

IRAN

Last modified 23 May 2019

LAW

Iran has not enacted comprehensive data protection legislation. However, several laws and regulations incorporate data protection provisions.

These include:

- Sharia law principles
- The Constitution of the Islamic Republic of Iran
- Draft of the Bill on Protection of Data and Privacy in the Cyber Space 2018
- Charter of Citizen's Rights 2016
- Cyber Crime Act 2011
- The Law Concerning Protection of Consumers Rights 2010
- The Law on Publishing and Access to Data 2010
- Stock Market Law 2006
- Electronic Commerce Law (ECL 2004)
- The Law on Facilitation of Competition and Prevention of Monopoly 2004
- The Law on respect for Legitimate Rights and Citizen Rights 2004
- The Law on Establishment of the Ministry of Justice Official Experts 2003
- Press Law 2001
- Criminal Code 1997
- Bylaw Concerning Official Translators 1996
- Criminal Procedures Code 1994
- Direct Taxation Act as amended 1988
- The Law on Statistic Centre of Iran1976
- Civil Liability Code 1960
- The Law on Establishment of Notary Public Offices 1937
- Iranian Bar Association Law 1936

DEFINITIONS

Definition of Personal Data

Not specifically defined.

Under the Law on Publishing and Access to Data, "personal data" means first and last name, home and work address, individual habits, bank accounts information, etc.

The E-Commerce Law defines "private data" as a "data message" associated with a specific data subject. "Data message" means

any representation of facts, information, and concepts generated, sent, received, stored or processed by use of electronic, optical or other information technology means.

Definition of Sensitive Personal Data

Not specifically defined.

Under the E-Commerce Law "sensitive personal data" has customarily been understood to mean data relating to family matters, criminal records, tribal or ethnic origins, moral and religious beliefs, ethical characteristics, sexual habits and data regarding health, physical or psychological status.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in Iran.

REGISTRATION

There is no registration requirement.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

Data collection and processing, including publication, is subject to data subject consent, provided that the "data message" is otherwise in accordance with Iranian law.

The collection and processing of personal "data messages" via electronic means is subject to the following conditions:

- the purpose of collection and processing must be specified and clearly described
- data may only be collected to the extent necessary to achieve its purported purpose
- "data messages" must be correct and up-to-date
- data subjects must be provided with access to computer files that contain "data messages" that concern the data subject
- data subjects must be provided with the ability to delete or rectify "data messages," in accordance with relevant regulations (Article 59, E-Commerce Law)

Unless otherwise provided by law, the following is prohibited: searching, collecting, processing, using or disclosing personal data. This prohibition also applies to other mail and telecommunications, including telephone communications, faxes, wireless and private internet communications.

TRANSFER

The Charter of Citizen's Rights prohibits personal data transfers without express data subject consent.

Under the ECL, third party and extraterritorial data transfers are subject to:

- data subject consent
- assurance that adequate security levels are in place to protect personal data in accordance with data subject rights and freedoms

SECURITY

Generally, Iranian business are required to take reasonable measures to secure personal information. It is unclear whether such measures must be physical, technical or organizational.

Nevertheless, somehow effective regulations apply to some businesses which are involved in sensitive information such as judges,

attorneys, doctors, hospitals and pharmacies.

Under the ECL, "secure information system" is defined as an information system that:

- is reasonably protected against misuse or penetration
- possesses a reasonable level of proper accessibility and administration
- is reasonably designed and organized in accordance with the significance of the task
- is in compliance with secure methods

A "secure method" is a method to authenticate "data message" date, correctness, origin and destination, as well as to detect errors and modifications in its communication, content, or storage from a certain point. A secure message is generated using algorithms or codes, identification words or numbers, encryption, acknowledgement call-back procedures or similar secure techniques.

BREACH NOTIFICATION

There is no requirement to report data breaches to any individual or regulatory body.

ENFORCEMENT

Iranian courts generally enforce violations through statutorily defined remedies of the applicable law or regulation.

For example, the Cyber Crime Act provides that anyone who, by use of computer or telecommunication means, publicizes or makes accessible another individuals film, pictures or sounds, or personal or family secrets without consent, and causes loss or damage to the individual or violates that person's dignity will be sentenced to imprisonment between 61 days and six months or fined Rls 1,000,000 to 10,000,000.

ELECTRONIC MARKETING

There is no specific electronic marketing law in Iran. However, under the Charter of Citizen's Rights, operators must obtain addressee consent before sending any advertisement. Personal cell phones are considered as a private zone. Sending any unwanted advertisements, or spam, is against the law.

ONLINE PRIVACY

There is no specific online privacy law in Iran.

KEY CONTACTS

Dr. Hassan Sedigh
CEO
Sedigh & Associates Petroleum Consultants
T +98 21 22009042 - 3
sedigh@sa-petroleum.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

IRELAND

Last modified 11 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

Irish data protection law underwent a significant overhaul with the introduction of the Data Protection Act 2018 (the 'Act'). The Act implements Directive (EU) 2016/680 (the 'Directive') and gives further effect to Regulation (EU) 2016/679 (the General Data Protection Regulation or the 'GDPR') in the areas in which Member State flexibility is permitted. The Act largely repeals the current Data Protection Acts 1988 and 2003 (the 'DPA') except for the purposes of national security, defence and the international relations of the state.

For contexts falling under the GDPR, the Act may be cited as the Data Protection Act 2018. For contexts involving the security, defence and international relations of the State, the Act and DPA may be cited together as the Data Protection Acts 1988 to 2018.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location

data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions contained within the Act are identical to those in the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Section 10 of the Act establishes a body known as *An Coimisinéir Cosanta Sonraí* (or the Data Protection Commission) (the 'Commission') and transfers the functions of the current Data Protection Commissioner to the Commission. The Commission will consist of between one and three members, the number of which shall be determined by the Government. These members will be known as Commissioners. In the event that there is more than one Commissioner, one Commissioner will be appointed as a Chairperson. The Chairperson will have the casting vote in the event of a tie.

The contact details of the Data Protection Commission (or *An Coimisinéir Cosanta Sonraí*) are as follows:

Dublin Office:
21 Fitzwilliam Square, Dublin 2, D02 RD28, Ireland

Regional Office:
Canal House, Station Road, Portarlington, R32 AP23 Co. Laois

Telephone: +353 57 868 4800 or +353 761 104 800

Website: www.dataprotection.ie

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Under the DPA, certain categories of data controller or data processor were required to register with the Data Protection Commissioner, except in a limited number of circumstances. This requirement no longer exists. Therefore a data controller or processor does not have to inform the Commission of their role and does not have to be entered onto a register.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;

- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

Section 34 of the Act enables the Minister, following consultation with such other Minister of the Government as he or she considers appropriate and the Commission, to make regulations requiring controllers, processors, or associations or other bodies representing categories of controllers or processors to designate a data protection officer.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organisations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily

accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

In accordance with the scope given to Member States under the GDPR, the Act permits exceptions to the prohibition on processing personal data and special categories of personal data for purposes other than for which they were collected. These further purposes include processing where necessary: to prevent a threat to national security, defence, or public security; to prevent, detect, investigate, or prosecute criminal offences; and for exercising or performing any right or obligation under employment or social welfare law. The Act also specifies the lawfulness of processing for select purposes including: establishing, exercising or defending legal rights; limited processing of political data in the course of electoral activities in the State; the administration of justice; insurance and pension purposes; preventative and occupational medicine; public health; archiving purposes; and, in certain circumstances, personal data relating to criminal convictions and offences. Under the Act, the digital age of consent in Ireland has been set at age 16 years.

The Act sets out examples of 'suitable and specific measures' that may be taken as appropriate to safeguard the fundamental rights and freedoms of data subjects when processing the personal data of data subjects. These measures are already either explicitly or implicitly contained in the GDPR:

- explicit consent
- limitations on access to the personal data undergoing processing within a workplace
- strict time limits for the erasure of personal data and mechanisms to ensure that such limits are observed
- specific targeted training for those involved in processing operations
- having regard to the state of the art, the context, nature, scope and purposes of data processing and the likelihood of risk to, and the severity of any risk to, the rights and freedoms of data subjects:
    - logging mechanisms to permit verification of whether and by whom the personal data have been consulted, altered, disclosed or erased
    - in cases in which it is not mandatory under the Data Protection Regulation, designation of a data protection officer
    - where the processing involves data relating to the health of a data subject, a requirement that the

processing is undertaken by a health care practitioner, or a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health practitioner
- pseudonymisation of the personal data, and
- encryption of the personal data

The Act also sets out that special categories of personal data, identical to those in the GDPR, may be processed subject to the suitable and specific measures outlined above for select purposes, including: to prevent treats to national security, defence or public security; to prevent, detect, investigate or prosecute criminal offences; employment and social welfare law; legal advice and legal proceedings; electoral activities and functions of the Referendum Commission; administration of justice and performance of conferred functions; for insurance and pension purposes; for reasons of substantial public interest; for purposes of Article 9(2)(h) GDPR; for public interest in the area of public health; and for archiving in the public interest, scientific or historical research or statistical purposes.

The Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018 came into effect in August 2018 and will have a significant impact on the processing of personal data in Ireland for the purposes of health research, which is defined as "*scientific research for the purpose of human health*". Most notably, the Regulations provide that when processing personal data for the purposes of health research, the explicit consent of the data subject must be obtained, except in limited circumstances where a declaration that such consent is not required is made by a committee established under the Regulations. Where a controller is procesing personal data for health research purposes, it must ensure certain specified "suitable and specific measures are taken to safeguard the fundamental rights and freedoms of the data subject". These overlap with, and in some cases go beyond, what is explicitly required under the GDPR and the Act and include:

- having arrangements in place so that personal data will not be processed in a way that causes, or is likely to cause, damage or distress; and
- having appropriate governance structures and processes and procedures in place for carrying out the health research.

The Data Protection (Amendment) Bill 2018, introduced in November 2018, proposes to amend the Act in order to protect a child's personal data from being processed for marketing purposes. The Bill is currently before Dáil Éireann (the lower house of the legislature in Ireland) at the second stage of the legislative procedure.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU - U.S. Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject

between the controller and another natural or legal person;

d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The GDPR provides flexibility for Member States to set limits on the transfer of specific categories of personal data to third countries or international organisations. Excluding law enforcement purposes, the Act has not directly set such limits, but provides that the Minister for Justice, following consultation with other Ministers of Government as he or she considers appropriate, and the Commission may make regulations restricting the transfer of categories of personal data to a third country or an international organisation for important reasons of public policy. Any such regulations may be expressed to apply to one or more of:

- a category or categories of personal data
- a third country or class of third countries, or
- an international organisation

Transfers of personal data to third countries or international organisations for law enforcement purposes are dealt with extensively, but this is in pursuance to the Directive, and not the GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The security measures set out in the Act reflect those set out in the GDPR.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Act does not build further on the GDPR's breach notification requirements or procedures.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;

- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Under the Act the enforcement of data protection law in Ireland is the responsibility of the Commission. The Commission will have responsibility for enforcement of domestic matters but may also be responsible for matters which are pan-European. This would be the case where the Commission is selected as the lead supervisory authority under the 'one-stop-shop' principal under the GDPR.

The Act significantly increases the Commission's ability to enforce data protection law by giving it the following powers:

1. to order a controller or processor to comply with data subject requests
2. to order rectification or erasure of personal data or restriction of processing of personal data
3. to order a controller to communicate a personal data breach to data subjects
4. to issue enforcement notices that require a controller or processor to take such steps as the Commission considers necessary and appropriate
5. to require a report on any matter specified in the enforcement notice served on the controller or processor, or require production of any statement, record, or document pursuant to any provision of European or Irish privacy and data protection laws
6. to audit the practices and procedures of a controller or processor
7. to require production of any documents, records, statements or other information within a controller or

processor's control that are relevant to or required for the audit

8. to carry out an investigation for the purposes of an inquiry into suspected infringement
9. to impose administrative fines in addition to or instead of other enforcement measures.

The final point (9) is highly significant. The Act provides that the Commission can impose administrative fines of up to €20 million or 4% of global turnover, whichever is higher. In the case that the subject of an administrative fine be a public body that does not act as an undertaking within the meaning of the Competition Act 2002, the administrative fine may not exceed €1,000,000. In comparison to the DPA, the Act greatly enhances the Commission's ability to enforce compliance by controllers and processors.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The ePrivacy Regulations implement the anti-spam rules set out in Article 13 of the Privacy and Electronic Communications Directive 2002/58/EC (as amended by the Citizens' Rights Directive). These regulations came into effect on 1 July 2011. Electronic mail includes text messages (SMS), voice messages, sound messages, image messages, multimedia message (MMS) and email messages.

Direct marketing emails can generally only be sent to users with their prior consent. A limited exemption is available for direct marketing emails sent to existing customers promoting other products or services similar to those previously purchased by that consumer (such emails can only be sent for 12 months, the customer must have been given the opportunity to object when the details were collected and the product or service being marketed must be a product or service offered by the person with the existing relationship with the customer). B2B direct marketing emails can generally be sent unless the recipient has informed the sender that it does not consent to the receipt of such messages.

The identity of the sender must not be disguised or concealed and the recipient must be offered an opt-out.

Direct marketing calls (excluding automated calls) may be made to a landline provided the subscriber has not previously objected to receiving such calls or noted his or her preference not to receive direct marketing calls in the National Directory Database. Direct marketing calls cannot be made to a mobile phone without prior consent.

One cannot send a direct marketing fax to an individual subscriber in the absence of prior consent. One can send such a fax to a corporate subscriber unless that subscriber has previously instructed the sender that it does not wish to receive such communications or has recorded a general opt-out to receiving such direct marketing faxes in the National Directory Database.

Breach of these anti-spam rules is a criminal offence. On a summary prosecution (before a judge sitting alone) a maximum fine of EUR 5,000 per message sent can be handed down. On conviction on indictment (before a judge and jury) a company may be fined up to EUR 250,000 per message sent and an individual may be fined up to EUR 50,000 per message.

Electronic marketing is not directly dealt with by the GDPR and the Act follows suit. In Ireland, electronic marketing is currently governed by the ePrivacy Directive (Directive 2002/58/EC), implemented in Ireland by the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (the '2011 Regulations'). The proposed new ePrivacy Regulation, currently in draft form, will replace these. The proposed ePrivacy Regulation is intended to be read in light of the GDPR.

ONLINE PRIVACY

Cookies

Consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user. The 2011 Regulations expressly refer to the use of browser settings as a means to obtain consent. There is no express requirement for consent to be 'prior' to the use of a cookie. A user must be provided with 'clear and comprehensive information' about the cookie (including, in particular, its purposes). This information must be prominently displayed and easily accessible. The methods adopted for giving information and obtaining consent should be as 'user friendly' as possible.

The DPC has provided regulatory guidance on the use of cookies which can be accessed here.

Location Data

One cannot process location data unless either:

- such data has been made anonymous, or
- user consent has been obtained.

A provider of electronic communication networks or services or associated facilities (ie a telco) must inform its users of:

- the type of location data (other than traffic data) that will be processed
- the purpose and duration of the processing, and
- whether the data will be transmitted to a third party to provide a value added service. Users can withdraw their consent to the processing of location data.

Cookies

Cookie data is not dealt with by the GDPR, and the Act also does not address this topic. Cookie usage is instead dealt with by the 2011 Regulations. The proposed new ePrivacy Regulation, currently in draft form, will replace these. The proposed ePrivacy Regulation is intended to be read in light of the GDPR.

Location Data

Location data is captured by the GDPR within the definition of personal data. The Act does not specify any additional requirements for processing such personal data.

KEY CONTACTS

Mason Hayes & Curran
www.mhc.ie/

Philip Nolan
Partner and Head of Commercial Department
T +353 1 6145078
pnolan@mhc.ie

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ISRAEL

Last modified 28 January 2019

LAW

The laws that govern the right to privacy in Israel are the Basic Law: Human Dignity and Liberty, 5752 - 1992; the Protection of Privacy Law, 5741-1981 and the regulations promulgated thereunder (the PPL); and the guidelines of the Israel Privacy Protection Authority.

DEFINITIONS

Definition of Personal Data

Personal data, as defined under the PPL, means: data regarding the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person.

Definition of Sensitive Personal Data

Sensitive data, as defined under the PPL, means: data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person; and other information if designated as such by the Minister of Justice with the approval of the Constitution, Law and Justice Committee of the Knesset. No such determination has been made to date.

NATIONAL DATA PROTECTION AUTHORITY

The Israel Privacy Protection Authority (**PPA**), established in September 2006, as determined by Israel's Government decision no. 4660, dated January 19, 2006.

REGISTRATION

Subject to certain exceptions, database registration is required to the extent one of the following conditions are met:

- The database contains information in respect of more than 10,000 data subjects
- The database contains sensitive information
- The database includes information on persons, and the information was not provided by them, on their behalf or with their consent
- The database belongs to a public entity
- The database is used for direct-marketing services

Subject to certain exceptions, a database is defined under the PPL as a collection of data, stored by magnetic or optic means and intended for computer processing, consequently excluding non-computerized collections.

In 2005, the Ministry of Justice set up a committee generally known as the 'Schoffman Committee' which recommended relaxing registration of ordinary databases and focusing on specific categories of information (eg, medical data, criminal records or information about a person's political or religious beliefs). However, to date, the Schoffman Committee recommendations have not crystallized into binding legislation.

On November 28, 2018, the IPA published a statement of opinion regarding collection of email addresses. The statement asserts that the provisions applicable to databases under the PPL also would apply to a computerized list containing a collection of email addresses alongside their owners' names.

DATA PROTECTION OFFICERS

Appointment of a Data Protection Officer is required by an entity meeting one of the following conditions:

- Possessing five databases that require registration
- Being a public body as defined in section 23 to the POPL
- Being a bank, insurance company or a company engaging in rating or evaluating credit

Failure to nominate a Data Protection Officer when required to do so may result in criminal sanctions, including administrative fines. The PPL does not require that the Data Protection Officer be an Israeli citizen or resident.

If a company appoints a data protection officer pursuant to the PPL, then Israel Protection of Privacy Regulations (Data Security), 5777-2017 (Data Security Regulations) require that the officer be directly subordinate to the database manager, or to the manager of the entity that owns or holds the database. In addition, the Data Security Regulations prohibit the officer from being in a conflict of interest and require the officer to establish data security protocols and ongoing plans to review compliance with the Data Security Regulations. The officer must present findings from such review to the database manager and its supervisor.

COLLECTION & PROCESSING

The collection, processing or use of personal data is permitted subject to obtaining the informed consent of the data subjects. Such consent should adhere to purpose, proportionality and transparency limitations. As such, consent should be obtained for specific purposes of use, the processing and use of personal data should be proportionate to those purposes, and data subjects should have the right to inspect and correct their personal data. The data subject's consent must be re-obtained for any change in the purpose of use.

Any request for consent from a data subject to have his or her personal data stored and used within a database must be accompanied by a notice indicating:

- Whether there is a legal requirement to provide the information
- The purpose for which the information is requested
- The recipients of the data, and
- The purpose(s) of use of the data

Retaining outsourcing services for the processing of personal data is subject to the PPA's Guidelines on the Use of Outsourcing Services of Processing Personal Information (Guideline 2 2011) dated June 10, 2012 (Outsourcing Guidelines). The Outsourcing Guidelines include, inter alia, factors to be taken into consideration when deciding to use outsourcing services, specific provisions to be included within the data transfer agreement, and data security requirements. Processing of personal data in certain sectors is subject to additional outsourcing requirements.

The Outsourcing Guidelines require compliance with the Data Security Regulations.

Entities subject to separate outsourcing guidelines are, for example, entities supervised by the Commissioner of the Capital

Market, Insurance and Savings, and entities supervised by the Banking Supervision Department of the Bank of Israel. On February 27, 2018, the PPA published draft guidelines regarding the applicability of the Data Security Regulations to managing companies and insurers supervised by the Israel Capital Market, Insurance and Savings Authority. The draft guidelines state that supervised organizations that are subject to and comply with the Israel Capital Market, Insurance and Savings Authority information security directives will be deemed compliant with the Data Security Regulations upon meeting specific conditions set forth in the draft guidelines. On September 10, 2014, the Banking Supervision Department of the Bank of Israel issued draft guidelines regarding risk management in cloud computing services used by Israeli banking corporations. The guidelines were recently revised (November 13, 2018) to revoke the obligation on supervised entities to receive the approval of the Supervisor of Banks prior to using cloud computing services. However, the Supervisor of Banks has not lifted the ban on using cloud computing services for core activities and core systems.

The general issue of privacy consideration in the use of surveillance cameras is governed by the IPA Use of Security and Surveillance Cameras and the Footage Obtained Therein Guidelines (no. 4/2012, dated October 21, 2012). The IPA published additional supplementary Guidelines (no. 5/17, dated October 17, 2017), specifically referring to the use of surveillance cameras in the workplace. The draft guidelines state that the employer's prerogative to use surveillance means in the workplace is subject to the fulfillment of principals such as legitimacy, transparency, proportionality, good faith and fairness. These principles also apply to businesses required by law enforcement to place surveillance cameras on their premises. The guidelines specify the manner in which these principles should be implemented, derivative requirements and possible implications. Recently (July 5, 2018), the PPA published its position specifically addressing the use of surveillance cameras in kindergartens. The PPA position provides that an organization must seek legal advice and conduct a comprehensive examination of whether the installation of cameras is necessary to the protection of children, and whether the resulted infringement of privacy will not exceed the potential benefit from such installation.

TRANSFER

The transfer of personal data abroad is subject to the Privacy Protection Regulations (Transfer of Data to Databases Abroad), 5761-2001, pursuant to which personal data may be transferred abroad only to the extent that:

- The laws of the country to which the data is transferred ensure a level of protection, no lesser than the level of protection of data provided for by Israeli Law, or
- One of the following conditions is met:
    - The data subject has consented to the transfer
    - The consent of the data subject cannot be obtained and the transfer is vital to the protection of his or her health or physical well-being
    - The data is transferred to a corporation under the control of the owner of the database from which the data is transferred, provided that such corporation has guaranteed the protection of privacy after the transfer
    - The data is transferred to an entity bound by an agreement with the database owner, to comply with the conditions governing the use of the data as applicable under Israeli Laws, mutatis mutandis
    - Data was made available to the public or was opened for public inspection by legal authority
    - Transfer of data is vital to public safety or security
    - The transfer of data is required by Israeli Law
    - Data is transferred to a database in a country:
        - Which is a party to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Sensitive Data, or
        - Which receives data from Member States of the European Community, under the same terms of

acceptance, or

- In relation to which the Registrar of Databases announced, in an announcement published in the Official Gazette (Reshumot), that it has an authority for the protection of privacy, after reaching an arrangement for cooperation with that authority

When transferring personal data abroad, the database owner is required to enter into a data transfer agreement with the data recipient, pursuant to which the recipient undertakes to apply adequate measures to ensure the privacy of the data subjects and guarantees that the data shall not be further transferred to any third party.

The foregoing data transfer agreement must also comply with additional restrictions, to the extent that the recipient provides outsourcing services, as set forth in the Outsourcing Guidelines.

On January 31, 2011, the European Commission, on the basis of Article 25(6) of directive 95/46/EC, determined that the State of Israel ensures an adequate level of protection with regard to automated processing of personal data.

Additionally, the transfer of databases is subject to the IPA Draft Guidelines No. 3/2017 dated August 13, 2017, regarding the interpretation and implementation of the provisions of the PPL further to transfer of ownership of databases and its implications on data subject rights, which under certain circumstances, such as database recipient having a conflict of interest, might require opt-in consents from data subjects as a condition to transferring databases.

SECURITY

On March 21, 2017, the Constitution, Law, and Justice Committee of the Knesset approved the Data Security Regulations, which came into effect in May 2018. The Data Security Regulations specify the manner in which the general information security requirements under the PPL are to be implemented. The Data Security Regulations further broaden the PPL by imposing additional requirements applicable to database owners (controllers), holders (processors) and managers. Such additional requirements include, without limitation, the creation and implementation of a broad list of manuals, policies, practices and documents, such as: Database Definitions Document; Data Security Protocol; Database Mapping Document; Database Inventory; Valid Authorization List (including all authorized access personnel, titles, and database access level); Mobile Device Policy; Backup Policy and Recovery Procedure Document); and others; various physical, environmental and logical security measures; and regular audit, inspection and training obligations. The requirements under the Data Security Regulations are categorized in accordance with the level of sensitivity (high / medium / low) of the database.

The Data Security Regulations add to the Outsourcing Guidelines, which in effect expand the requirements applicable when outsourcing processing services, even prior to entering into a data transfer agreement between the database owner and the data recipient and the requirements to be included therein.

Failure to comply with the Data Security Regulations will constitute a breach of the PPL, which may expose a noncompliant entity to criminal and civil liability, as well as to administrative fines.

On September 2, 2018, the IPA published, by virtue of its cross-supervision authority, audit questionnaires in respect of personal information managed or maintained in databases. Organizations that manage or maintain such information are required to answer the questionnaires for the purpose of assessing their compliance with the provisions of the PPL and regulations promulgated thereunder, inter alia, regarding the manner of obtaining data subjects consent to use the information, the types of use of such information and the processing and security measures taken with respect thereof.

BREACH NOTIFICATION

Pursuant to the Data Security Regulations, data breach notifications are required depending on the severity of the breach and the level of security of the database. Such notifications are generally provided to the IPA which may require further notification to the data subjects.

Along with the publication of the Data Security Regulations, the PPA published its policy regarding the applicable notification obligations pursuant to a data breach and the IPA's discretion in enforcement of such obligations.

ENFORCEMENT

PPA has the authority and obligation to supervise compliance and enforce the provisions of the PPL and appoint inspectors to carry out those activities.

Breach of the PPL may result in both civil and criminal sanctions, including administrative fines, one to five years of imprisonment and the right to receive statutory damages under civil proceedings without the need to prove actual damages.

On January 21, 2018, the Israeli Ministerial Committee for Legislation approved a draft bill for the 13th Amendment of the PPL for broadening the PPA's enforcement powers. The current draft bill provides IPA with the ability to conduct criminal investigations and to impose monetary sanctions in the amount of up to 3.2 million. The draft bill passed its first reading in the Knesset in March 2018 but has yet to pass the approval of the Knesset Constitution, Law and Justice Committee; thereafter it would need to also pass the second and third readings in the Knesset, in order to become a binding piece of legislation.

ELECTRONIC MARKETING

Unsolicited marketing is regulated under the Communications Law (Telecommunications and Broadcasting), 5742-1982 (the Anti-Spam Act). The Anti-Spam Act prohibits, subject to certain exceptions, automated messaging sent electronically via email, automatic dialing system, fax or text messages, mainly for marketing and promotional purposes, without first obtaining the recipient's initial opt-in prior consent; all such communications also must contain an opt-out or an unsubscribe option.

The PPL governs the possession and management of databases intended for direct mailing and direct mailing services. Direct mailing is defined in Section 17C of the PPL as personally contacting a person, based on his belonging to a group of the population that is determined by one or more characteristics of the data subjects listed in the database. Direct mailing services are also defined in the same Section as providing direct mailing services to others by way of transferring lists, labels or data by any means. The PPL imposes restrictions in connection therewith, including without limitation: mandatory notification requirements in respect of the registered database number; the identity and contact details of the respective database owner; the source of the data; database registration requirement (regardless of the number of data subjects listed or the sensitivity of the data), specifying the purpose of direct mailing; specific record-keeping requirements; compliance with data subjects' rights of access, rectification and deletion of data from the database or banning its onward transfer.

The IPA Guidelines No. 2/2017 for the interpretation and implementation of the PPL provisions with respect of direct mail and direct mail services, intends to clarify these additional restrictions and stricter regulations with respect of direct mailing and direct mailing services. Additionally, the said IPA Guidelines govern direct marketing services which, inter alia, require specific opt-in consents and notice requirements.

ONLINE PRIVACY

The PPL does not specifically address online privacy, cookies and / or location data, all of which are governed by the general restrictions detailed above, including the requirements imposed on processing databases, direct marketing and the consent, purpose and proportionality restrictions.

The PPL governs information "about a person." As such, depending upon the circumstances at hand, any non-identifiable and anonymous information (which cannot be re-identified) may reasonably be interpreted as falling outside the confines of the PPL limitations.

KEY CONTACTS

Goldfarb Seligman & Co., Law Offices
www.goldfarb.com

Sharon Aloni
Partner
T +972 (3) 608 9834
sharon.aloni@goldfarb.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ITALY

Last modified 10 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Italian data protection law framework has been harmonized with the GDPR by means of the Legislative Decree 101/2018, that entered into force on 19 September 2018, amended a number of provisions of the Legislative Decree 196/2003 (the "**Privacy Code**"), as well as introduced some transitional provisions regulating the migration to the new regime.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data

relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Italian Privacy Code adopts the definitions provided by the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Privacy Code provides that the supervisory authority in Italy is the Garante per la protezione dei dati personali (the "**Garante**"). The Garante is composed of a Council and an Office. The Council is made up of four members, two elected by the Chamber of Deputies and two by the Senate of the Republic. The members are elected amongst those who apply for this position in a selection procedure whose details are published on the websites of the Chamber of the Deputies, the Senate of the Republic and the Garante. The members elect a Chairman, in the event of parity of votes. The Office is made up of 162 members that are recruited by way of a public competition.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Under the GDPR and the Privacy Code there is no obligation to notify regulators of any data processing activity.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which

the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organisations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Privacy Code provides several restrictions on data subjects' rights for reasons of justice. In particular, data subjects rights may be exercised within the limits established in the law and regulations on the proceeding and procedures before the courts.

Furthermore, the Privacy Code sets out data protection rights of deceased persons. Indeed, the rights provided for in Articles 15 through 22 of the GDPR referring to personal data concerning deceased persons may be exercised by those having an interest of their own, or act to protect the data subject, as her/his delegate, or for family reasons worthy of protection. The exercise of such rights is not permitted when provided for by the law or when, specifically limited to the offer of information society services, the data subject expressly prohibited it in writing by way of a declaration sent to the data controller. The data subject may withdraw or modify such declaration at any time.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU - U.S. Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Privacy Code does not derogate from the GDPR in regard to transfers.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The Privacy Code does not prescript further security measures that should be followed to protect personal data.

Nevertheless, genetic data, biometric data or data concerning health must be processed in accordance with the additional safeguard measures issued by the Garante every two years (Section 2-*septies*). Such safeguard measures take into account the guidelines, recommendations and best practices published by the European Data Protection Board and best practices on personal data processing; scientific and technological evolution in the sector covered by such measures; and the interest of the free flow of personal data within the territory of the Union. Also, the Garante may issue codes of ethics that set out security measures for the processing of personal for statistical and scientific research purposes.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Privacy Code does not set out additional rules on data breach notifications.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The Privacy Code provides that investigations and enforcement actions handled by the Garante.

ELECTRONIC MARKETING

The GDPR and the Privacy Code apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). As further analyzed below, under Section 130 of the Privacy Code, the legal basis for electronic marketing is consent. The strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Privacy Code (Section 130) does not prohibit the use of personal data for the purpose of electronic marketing, but it requires the prior informed consent (opt-in) from the recipient of the communication. The use of automated calling or communications systems without human intervention for the purposes of direct marketing or for sending advertising materials, or else for carrying out market surveys or interactive business communication, as well as electronic communications performed by e-mail, facsimile, MMS or SMS-type messages or other means shall only be allowed with the contracting party's or user's consent. Such consent shall be recorded with reference to its date and the person giving it in order to be used as evidence of the consent.

Separate consents shall be required for the registration to a website and the opt-in to the delivery of marketing communications, however the data subjects may be required to provide a unique marketing consent covering the different marketing practices (e.g. marketing via SMS, email, telephone, market surveys, etc.) performed through the collected data, provided that such practices are outlined in the information notice provided to data subjects.

An additional separate consent shall be required for the transfer of collected personal data to third parties for marketing purposes. Said third party shall also be identified at least on the basis of its category of operation and provide an information notice to data subjects before the delivery of marketing communications.

Where a data controller uses, for direct marketing of his own products or services, electronic contact details for electronic mail supplied by a data subject in the context of the sale of a product or service, said data controller may fail to request the data

subject's consent, on condition that the services are similar to those that have been the subject of the sale and the data subject, after being adequately informed, does not object to said use either initially or in connection with subsequent communications. The data subject shall be informed of the possibility to object to the processing at any time, using simple means and free of charge, both at the time of collecting the data and when sending any communications for the purposes here referred.

Electronic marketing communications shall clearly identify the sender and provide to the recipient all necessary information in order for him/her to eventually refuse the delivery of the direct marketing material (*opt-out*).

The possibility for the recipient to opt-out from marketing communication services must be guaranteed both during the first contact with the recipient and during any following communications.

Marketing communications by way of non-automated telephone calls are permitted provided that either:

- the data subject has given his prior consent, or
- the number of the data subject is included in the telephone directory and (s)he has not entered in a public opt-out register ("*Registro delle Opposizioni*") and opted out from being contacted for marketing purposes.

Law 11 January 2018, no. 5 provides stringent rules on telemarketing, including, amongst others, the withdrawal from all consents previously given in case of enrolment in the *Registro delle Opposizioni*, save for consents provided based on contractual arrangements in place or expired less than 30 days before the enrolment, and the prohibition to communicate, transfer or disseminate personal data related to data subjects registered in the *Registro delle Opposizioni* for advertising or sales purposes or for the purposes of carrying out market research or commercial communications not related to the activities, products or services offered by the data controller.

The above mentioned privacy provisions apply also to communications sent through private messages on social networks and through Voip. On the contrary, should the data subject be a follower of a social network page, it may be implied that the data subject has consented to the delivery of marketing communications of the page. Marketing messages concerning a given brand, product or service as sent by the company managing the relevant social network page may be considered to be lawful if it can be inferred unambiguously from the context or the operational arrangements of the relevant social network, also based on the information provided, that the recipient did intend in this manner to also signify his/her intention to consent to receiving marketing messages from the given company. However the delivery of marketing communications shall stop when the data subject unregisters from the page.

The Privacy Code provisions relating to marketing and commercial communications make reference to the 'contracting party's and user's consent' rather than to the 'data subject's consent', referring both to individuals and companies.

ONLINE PRIVACY

The Privacy Code regulates the collection and processing of traffic data and location data by the provider of a public communications network or publicly available electronic communications service and the use of cookies.

According to Section 123 of the Privacy Code, traffic data shall be erased or made anonymous when they are no longer necessary for the purpose of transmitting the electronic communication. However traffic data can be retained for a period not longer than 6 months for billing and interconnection payments purposes or, with the prior consent of the contracting party or user (which may be withdrawn at any time), for marketing electronic communications services or for the provision of value added services.

According to Section 126 of the Privacy Code, location data may only be processed if made anonymous or if the subscriber or user has been properly informed and (s)he has given her/ his prior consent (which can be withdrawn at any time).

According to Section 122 of the Privacy Code (which reflects recital 66 of the E-Cookies Directive 2009/136/EC and the amended Section 5, par. 3 of the Directive 2002/58/EC – as amended by Directive 2009/136/EC) the storing of information in the contracting party's or user's computer is only allowed if said contracting party or user has been properly informed and (s)he has given her/his consent.

KEY CONTACTS

Giulio Coraggio
Partner
T +39 02 80 6181
giulio.coraggio@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

JAPAN

Last modified 24 January 2018

LAW

The Act on the Protection of Personal Information ("APPI") regulates privacy protection issues in Japan and the Personal Information Protection Commission (the "PPC"), a central agency acts as a supervisory governmental organization on issues of privacy protection.

The APPI was originally enacted approximately 10 years ago but was recently amended and the amendments came into force on 30 May 2017.

DEFINITIONS

Definition of Personal Information

Personal information is information about a living individual which can identify a specific individual by name, date of birth or other description contained in such information. Personal Information includes information which enables one to identify a specific individual with easy reference to other information. According to the guidelines issued by the PPC, "easy reference to other information" means that a business operator can easily reference other information by a method taken in the ordinary course of business. If a business operator needs to make an inquiry of another business operator to obtain the "other information" and it is difficult for the business operator to do so, such a situation would not be considered an "easy reference to other information".

Personal information includes any "Personal Identifier Code". A Personal Identifier Code refers to certain types of data specified under a relevant cabinet order of the APPI, and includes biometric data which can identify a specific individual, or data in the form of a certain code uniquely assigned to an individual. Typical examples of such code would be passport numbers or driver's license numbers.

Definition of Sensitive Personal Information

Sensitive information includes information about a person's race, creed, social status, medical history, criminal record, any crimes a person has been a victim of, and any other information that might cause the person to be discriminated against. Obtaining sensitive information generally requires consent from the data subject. Additionally, the "opt out" option (discussed below) is not available for third party transfer for sensitive information-prior consent is basically required from the data subject to transfer the sensitive information to a third party.

Definition of Anonymized Information

"Anonymized information" refers to any information about individuals from which all personal information (i.e., the information that can identify a specific individual, including any sensitive information) has been removed and such removed personal information cannot be restoredby taking appropriate measures specified in the enforcement rules and the relevant PPC guidelines. As noted above, personal information includes personal identifier codes, so these must also be removed before information is considered anonymized.

If a business operator has sufficiently anonymized the information, it can be used beyond the purpose of use notified to the data subject and disclosed to third parties without requiring the consent of the data subjects. However, care must be taken in anonymizing the information before disclosure; a failure to completely sanitize the information could result in the disclosure of personal information. Additionally, before disclosing the anonymized information to a third party, a business operator must publicly state (likely in its privacy policy) the items of information (for example, gender, birth year and purchase history) included among the Anonymized Information, and the means by which it shares the Anonymized Information.

NATIONAL DATA PROTECTION AUTHORITY

The PPC has been tasked with providing many of the details necessary to interpret and enforce the APPI. The PPC issues guidelines for general rules for handling personal information, offshore transfer, confirmation and record requirements upon provision of personal data to third parties and creation and handling anonymized information.The PPC is neutral and independent, and it has the power to enforce the APPI. However, it will only have the right to perform audits and issue cease and desist orders; it will not have the power to impose administrative fines.

Personal Information Protection Commission

Kasumigaseki Common Gate West Tower 32nd Floor, 3-2-1, Kasumigaseki, Chiyoda-ku, Tokyo, 100-0013, Japan
TEL: +81-(0)3-6457-9680

https://www.ppc.go.jp/en/

REGISTRATION

Japan does not have a central registration system.

DATA PROTECTION OFFICERS

There is no specific legal requirement to appoint a data protection officer. However, some guidelines provide that specific employees should be assigned to control personal data (eg Chief Privacy Officer).

COLLECTION & PROCESSING

Specifying the Purpose of Use

When handling personal information, a business operator must specify to the fullest extent possible the purpose of use of the personal information ('Purpose of Use'). Once a business operator has specified the Purpose of Use, it must not then make any changes to the said purpose which could reasonably be considered to be beyond the scope of what is duly related to the original Purpose of Use. In addition, when handling personal information, a business operator shall not handle the information beyond the scope that is necessary for the achievement of the Purpose of Use without a prior consent of the individual. In other words, the use of the information must be consistent with the stated Purpose of Use.

Public Announcement of the Purpose of Use

The Purpose of Use must be made known to the data subjects when personal information is collected or promptly thereafter and this can be made by a public announcement (such as posting the purpose on the business operator's website). When personal information is obtained by way of a written contract or other document (including a record made in an electronic or magnetic format, or any other method not recognisable to human senses), the business operator must expressly state the Purpose of Use prior to the collection.

A business operator must 'publicly announce' or 'expressly show the Purpose of Use' in a reasonable and appropriate way.

According to the guidelines issued by the PPC, the appropriate method for a website to publicly announce the Purpose of Use of information collected, is a one click access on the homepage so that the data subject can easily find the Purpose of Use before submitting the personal information.

TRANSFER

Disclosing/Sharing Personal Data

Currently, Personal Data (meaning Personal Information stored in a database) may not be disclosed to a third party without the prior consent of the individual, unless the business operator handling the personal information adopts the opt-out method, provides an advance notice of joint use to data subjects, in the case of merger/business transfer or entrusting the handling of Personal Data to third party service providers.

Even disclosing the Personal Data within group companies is considered disclosing the Personal Data to a third party and consent must be obtained, unless it meets the requirements of joint use. The APPI also has permitted the "opt out" method, whereby a business operator can as a default disclose personal information to third parties, unless individuals opt out of allowing the business operator to do so. The APPI requires a business operator to preemptively disclose to the PPC, and the public or to the data subject of certain items listed below concerning opt out.

- the purpose of use includes the provision of such information to third parties and the method of such provision;
- the nature of the personal data being provided to third parties;
- the method by which personal data is provided to third parties;
- the matter that provision of such information to third parties will be stopped upon the request by the data subject; and
- the method for an individual to submit an opt out request to the company.

The APPI does not provide any examples of how best to obtain consent from individuals before sharing Personal Data. Generally, written consent should be obtained whenever possible. When obtaining consent it would be prudent to clearly disclose to the data subject the identity of the third party to whom the Personal Data will be disclosed, the contents of the Personal Data and how the third party will use the provided Personal Data.

The guidelines issued by the PPC provide the following examples as appropriate methods of obtaining the consent for disclosing Personal Data from the data subject:

- receipt of confirmation of the oral or written consent (including a record created by electronically or magnetically methods or any other method not recognizable to human senses) from data subject
- receipt of a consent email from data subjects
- the data subject's check of the confirmation box concerning the consent
- the data subject's click of a button on the website concerning the consent, and
- the data subject's audio input, or touch of a touch panel concerning the consents

If Personal Data is to be used jointly, the business operator handling personal information could, prior to the joint use, notify the data subjects of or publish the following:

- the fact that the Personal Data will be used jointly
- the item of the Personal Data to be disclosed
- the scope of the joint users
- the purpose for which the Personal Data will be used by them, and
- the name of the individual or business operator responsible for the management of the Personal Data.

Cross-border Transfer

Under the APPI, in addition to the general requirements for third party transfer, prior consent of data subjects specifying the receiving country is required for transfers to third parties in foreign countries unless the foreign country is white-listed under the enforcement rules of the APPI or the third party receiving Personal Data has established similarly adequate standards for privacy protection as specified in the enforcement rules of the APPI.

According to the enforcement rules of the APPI, "similarly adequate standards" means that the practices of the business operator handling the Personal Data are at least equal with the requirements for protection of Personal Data under the APPI or that the business operator has obtained recognition based on international frameworks concerning the handling of Personal Data.

According to the guidelines for offshore transfer, one of the examples of an acceptable international framework is the APEC CBPR system. As of yet, no white-listed countries have been specified under the rules by the PPC. The PPC published a circular stating that they are aiming to specify EU countries as white-listed countries by early 2018.

SECURITY

The APPI requires that business operators prevent the leakage of Personal Data. The APPI does not set forth specific steps that must be taken. The PPC guidelines suggest recommended steps that business operators should take to ensure that personal data is secure. These necessary and appropriate measures generally include 'Systematic Security Control Measures', 'Human Security Control Measures', 'Physical Security Measures' and 'Technical Security Control Measures'.

Guidelines often contain several specific steps or examples that entities subject to the guidelines must take with respect to each of the security control measures such as developing internal guidelines pertaining to security measures, executing non-disclosure contracts with employees who have access to Personal Data, protecting machines and devices and developing a framework to respond to instances of leakage.

BREACH NOTIFICATION

It is not legally required to report a data breach incident to the PPC or to notify the relevant data subjects. However, the PPC guidelines recommend that this notification be made and it is the market standard practice to report data breach incidents in Japan. Not doing so and instead having the breach discovered publicly would have a potentially massive negative impact on brand image and reputation in Japan.

In addition, the PPC guidelines suggest that companies (i) make necessary investigations and take any necessary preventive measures, and/or (ii) make public the nature of the breach and steps taken to rectify the problem and (iii) send a voluntary notice to the data subject of the breach or publish the data breach, if appropriate and necessary.

According to the PPC guidelines, if a factual situation demonstrates that the Personal Data which has been disclosed was immediately collected before being seen by any third party or not actually disclosed, (such as the case where the company has encrypted the data or otherwise secured the data in such a way that they it has become useless to third parties being in possession of such data), the notice to the PPC or any other relevant authority is not necessary.

ENFORCEMENT

If the PPC finds any violation or potential violation of the APPI, the PPC may request the business operator handling personal information to submit a report, conduct on-site inspection and request or order the business operator handling personal information to take remedial actions. If a business operator handling personal information does not submit the report and materials, or reports false information they will be subject to a fine of up to JPY 300,000. If a business operator handling personal information does not follow an order from the PPC they will be subject to a penalty of imprisonment for up to six months or a fine of up to JPY 300,000.

An unauthorized disclosure of Personal Information, for the benefit of the disclosing party or any third party, will be subject to a penalty of imprisonment for up to one year or a fine of up to JPY 500,000.

If the party making the disclosure is an entity, the parties subject to this penalty will be the relevant officers, representatives, or managers responsible for the disclosure as well as the entity, which is subject to the fine specified above.

ELECTRONIC MARKETING

The Act on Specified Commercial Transactions ('ASCT') and the Act on the Regulation of Transmission of Specified Electronic Mail ('Anti-Spam Act') regulate the sending of unsolicited electronic commercial communications.

Under the ASCT, which focuses on internet-order services, a seller is prohibited from sending email or fax advertisements to consumers unless they provide a prior request or consent (ie an opt-in requirement). The seller is also required to retain the records that show consumers' requests or consents to receive email or fax advertisements for 3 years for email advertisements

and 1 year for fax advertisements after the last transmission date of an email or fax advertisement to the consumer.

If a seller has breached any of these obligations regarding email advertisements, such seller will be potentially subject to fine of up to JPY 1,000,000.

Under the Anti-Spam Act, which broadly covers commercial emails (eg an invitation email from a social network service), there are several regulations on sending email advertisements as follows:

- the sender must retain records evidencing there was a request or consent to receive emails at least for 1 month after the last date the seller sent an email to the recipient
- for-profit entities or individuals engaged in business sending any email to advertise their own or another's business must obtain a request or consent to receive emails from intended recipients unless the recipient falls under certain exceptions (eg there is a continuous transaction relationship between a sender and a recipient) in the Anti-Spam Act
- an email is required to include a sender's email address or a URL so that recipients can send opt-out notices to the sender, and
- senders must not send emails to randomly generated email addresses (with the hope of hitting an actual email address) for the purpose of sending emails to a large number of recipients.

The relevant ministry may order a sender to improve the manner of email distribution if the sender violates the requirements noted above. If the sender violates an order issued by the ministry (other than one related to the retention obligation), the sender is subject to imprisonment for up to 1 year or a fine of up to JPY 1,000,000. In addition, the entity will be subject to fine of up to JPY 30,000,000 if an officer or an employee of the entity commits any violation mentioned above. If the sender violates an order issued by the minister with respect to the retention obligation, the sender will be potentially subject to fine of up to JPY 1,000,000. In addition, the entity will be subject to fine of up to JPY 1,000,000 if an officer or an employee of the entity commits the violation mentioned above.

ONLINE PRIVACY

There is no law in Japan that specifically addresses cookies. However, if the information obtained through cookies may identify a certain individual in conjunction with other easily-referenced information (eg member registration) and it is utilised (eg for marketing purposes), such Purpose of Use of information obtained through the use of cookies must be disclosed under the APPI.

KEY CONTACTS

Lawrence G. Carter
Partner
T +81 3 4550 2800
lawrence.carter@dlapiper.com

Keitaro Uzawa
Associate
T +81 3 4550 2800
keitaro.uzawa@dlapiper.com

Brian Caster
Associate
T +81 3 4550 2800
brian.caster@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

JERSEY

Last modified 28 January 2019

LAW

The Data Protection (Jersey) Law, 2018 (DPJL) and the Data Protection Authority (Jersey) Law, 2018 (DPAJL) came into force on May 25, 2018. These laws superseded the Data Protection (Jersey) Law 2005, which had been held to be adequate by the European Commission for the purposes of the European Data Protection Directive (Directive 95/46/EC) (see Commission Decision 2008/393/EC). This decision continues to apply pending a review of Jersey's adequacy (to be conducted under Article 45 of the European General Data Protection Regulation (GDPR)), which is expected to take place in 2020.

The DPJL and DPAJL provide a broadly equivalent regime to that under the GDPR.

DEFINITIONS

The DPJL defines 'data' as information that:

- Is processed by means of equipment operating automatically in response to instructions given for that purpose or is recorded with the intention that it should be processed by means of such equipment
- Is recorded as part of a filing system or with the intention that it should form part of a filing system, or
- Is recorded information held by certain public authorities

The DPJL defines 'personal data' as being any data relating to a data subject.

A 'data subject' is defined in the DPJL as an identified or identifiable, natural living person who can be identified, directly or indirectly, by reference to (but not limited to) an identifier such as:

- A name, an identification number or location data
- An online identifier (which may include an IP address, location data or any unique number or code issued to the individual by a public authority), or
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the person

Enhanced levels of protection in the DPJL and DPAJL are provided for 'special category' personal data.

'Special category personal data' is defined under the DPJL as personal :

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership
- Genetic or biometric data that is processed for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation, or
- Data relating to a natural person's criminal record or alleged criminal activity

Personal data may be processed by either a '**controller**' or a '**processor**'. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 1(1) DPJL). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the DPJL imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

NATIONAL DATA PROTECTION AUTHORITY

The DPAJL created a Data Protection Authority (the Authority) to oversee the DPJL. Save in respect of certain matters (in particular the issuing of a formal public statement in relation to data protection issues or the issuing of an administrative fine), its functions are delegated to the Information Commissioner.

REGISTRATION

Data controllers and processors who process personal data must currently inform the Information Commissioner (an online portal is available) of the following:

- The name and address of the data controller (including a Jersey resident representative if the data controller is outside Jersey)
- A description of the personal data being, or to be, processed by or on behalf of the data controller and the category or categories of data subject to which they relate
- A description of the purpose or purposes for which the data are being or are to be processed
- A description of the recipients (if any) to whom the data controller intends or may wish to disclose the data, and
- The names, or a description, of any countries or territories outside of Jersey to which (directly or indirectly) the data controller transfers, or intends or may wish to transfer, the data

A new notification and fee scheme is expected by May 2019, the details of which have not yet been provided.

In many ways, external accountability to the Information Commissioner via registration or notification is superseded in the DPAJL and DPJL by rigorous demands for internal accountability.

In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 14(3) DPJL), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request.

DATA PROTECTION OFFICERS

Data controllers and processors are required (Article 24 DPJL) to appoint a data protection officer if:

- Processing is carried out by a public authority (with the exception of courts acting in their judicial capacity)
- The core activities of the controller or the processor consist of processing operations that, by virtue of their nature, scope or purposes, require regular and systematic monitoring of data subjects on a large scale
- The core activities of the controller or the processor consist of processing special category data on a large scale, or
- It is otherwise required by law

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 24(3) DPJL). However, larger corporate groups may find it difficult in practice to operate with a single data protection officer. The data protection officer must be easily accessible to:

- All data subjects
- The Information Commissioner, and
- The controller or processor who appointed the officer, along with the controller's or processor's employees that carry out data processing

Data protection officers (DPOs) must have expert knowledge (Article 24(6) DPJL) of data protection law and practices, though it

is possible to outsource the DPO role to a service provider (Article 24(7) DPJL).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 25(1) DPJL), and the DPO must directly report to the highest management level of the controller or processor (Article 25(2) DPJL).

In addition, controllers and processers must:

- Ensure that the data protection officer operates independently and does not receive any instructions regarding the performance of those duties, other than to perform them to the best of the officer's ability and in a professional and competent manner (Article 25(1)(c) DPJL), and
- Not dismiss or penalize the data protection officer for performing his or her duties other than for failing to perform them to the best of the officer's ability and in a professional and competent manner (Article 25(1)(d) DPJL)

The specific tasks of the DPO are set out in Article 26 DPJL and include:

- Informing and advising on compliance with the DPJL, DPAJL and other applicable data protection laws
- Monitoring compliance with the law and with the internal policies of the organization, including assigning responsibilities, raising awareness and training staff
- Advising on and monitoring data protection impact assessments, where requested, and
- Cooperating and acting as point of contact with the Information Commissioner

COLLECTION & PROCESSING

Controllers are responsible for compliance with a set of core principles that apply to all processing of personal data. Under these principles, personal data must be (Article 8(1) DPJL):

- Processed lawfully, fairly and in a transparent manner in relation to the data ('lawfulness, fairness and transparency')
- Collected for specified, explicit and legitimate purposes and once collected, not further processed in a manner incompatible with those purposes ('purpose limitation')
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')
- Accurate and, where necessary, kept up-to-date, with reasonable steps being taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed ('storage limitation') and
- Processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')

Additionally, the controller is responsible for and must be able to demonstrate compliance with the above principles ('accountability') (Article 6(1)(a) DPJL).

Accountability is a core theme of the DPJL. Organizations must not only comply with the DPJL, but also be able to *demonstrate* compliance, perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving (and being able to demonstrate) accountability.

Legal Basis for Processing

The DPJL works slightly differently to the GDPR in terms of establishing a legal basis for processing.

Data controllers may collect and process personal data when any of a number of conditions are met (Article 9 and Schedule 2 DPJL). The most frequently relied upon are as follows:

- The consent of the data subject
- The processing is necessary for:

    - The performance of a contract to which the data subject is a party, or
    - The taking of steps at the request of the data subject with a view to entering into a contract
- The processing is necessary to comply with a data controller's legal obligations (other than one imposed by contract)
- The processing is necessary to protect the data controller's vital interests
- The processing is necessary for:
    - The administration of justice
    - The exercise of any functions conferred on any person by or under any enactment
    - The processing is necessary for taking legal advice or the establishment, exercise or defense of legal claims
    - The exercise of any functions of the Crown, the States or any public authority, or
    - The exercise of any other functions of a public nature with a legal basis in Jersey law to which the controller is subject and exercised in the public interest by any person
    - The processing is necessary for the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, unless:
        - The processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject, in particular where the subject is a child, or
        - The controller is a public authority, or
    - The processing is necessary for reasons of substantial public interest provided for by law and is subject to appropriate protections to protect the rights and interests of the data subject

Special Categories of Data

Where special category personal data is processed, at least one of a more restrictive list of conditions than those for personal data must be satisfied (Article 9 and Schedule 2 Part 2 DPJL). Unlike the GDPR, personal data may also be processed on the basis of the conditions for processing special category data. The most frequently relied upon bases for processing special category data are as follows:

- The explicit consent of the data subject
- The processing is necessary to comply with a data controller's legal obligations (other than one imposed by contract)
- The processing is necessary for the purposes of exercising or performing any right, obligation or public function conferred or imposed by law on the controller in connection with employment, social security, social services or social care
- The processing is necessary for taking legal advice or the establishment, exercise or defense of legal claims
- The processing is necessary for reasons of substantial public interest provided for by law and is subject to appropriate protections to protect the rights and interests of the data subject
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- The processing relates to personal data which are manifestly made public by the data subject
- The processing is necessary for archiving or research
- The processing is necessary for the prevention of unlawful acts (or malpractice / mismanagement)
- The processing is necessary for certain insurance-based purposes, or
- The processing is necessary for medical purposes and is undertaken by a health professional

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data *(ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected). This is potentially in conflict with the core principle of purpose limitation, which aims to ensure that the rights of data subjects are protected. The DPJL sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 13 DPJL)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are, it will be much harder to form the view that a new purpose is compatible)

- The possible consequences of the new processing for the data subjects, and
- The existence of appropriate safeguards

Transparency

The data controller must provide the data subject with "fair processing information" (Article 12 DPJL), which includes:

- The identity and contact details of the controller, and where applicable, the controller's representative
- The contact details of the data protection officer (if any)
- The purposes for which the data are intended to be processed and the legal basis for the processing
- An explanation of the legitimate interests pursued by the controller or by a third party, if the processing is based on those interests
- The recipients or categories of recipients of the personal data (if any)
- Where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and whether or not there is an adequate level of protection for the rights and freedoms of data subjects in that country or organization
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- Information concerning the rights of data subjects
- Where the processing is based on consent, the existence of the right to withdraw consent
- The existence of any automated decision-making and any meaningful information about the logic involved in such decision-making and the significance of any such decision-making for the data subject
- A statement of the right to complain to the Information Commissioner
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failing to provide such data
- Where the personal data are not obtained directly from the data subject, information identifying the source of the data
- Any further information that is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in limited circumstances. Controllers must provide information on action taken in response to requests within four weeks as a default, with a limited right for the controller to extend this period a further eight weeks where the request is onerous. These periods are slightly shorter than those set out in the GDPR.

Right of access (Article 28 DPJL)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 31 DPJL)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 32 DPJL)

Data subjects may request erasure of their personal data.

The right is not absolute; it only arises in a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 33 DPJL)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed other than for legal claims of the data subject or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 34 DPJL)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format.

Right to object (Article 21 DPJL)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is for a public function. Controllers will then have to suspend processing of the data until such time as they demonstrate 'compelling legitimate grounds' for processing that override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time (Article 36 DPJL).

The right not to be subject to automated decision taking, including profiling (Article 38 DPJL)

Automated decision-making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

1. Necessary for entering into or performing a contract
2. Authorized by Jersey law or by the law of another jurisdiction in the British Isles or by EU or member state law, or
3. The data subject has given their explicit consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the controller must implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, including the right to obtain human intervention on the part of the controller, so that the data subject can express his or her point of view and contest the decision.

Children's consent to information society services (Article 11(4))

Article 11(4) of the DPJL stipulates that a child may only provide his or her own consent to processing in respect of information society (primarily, online) services, where that child is over 13 years of age. Otherwise, a parent (or other responsible adult) must provide consent on the child's behalf.

Processing agreements

The rules on agreements (or other legally binding instruments) between controllers and processors have been significantly enhanced.

The controller must appoint the processor in the form of a **binding written agreement** that sets out:

- The **subject matter** and **duration** of the processing
- The **nature** and **purpose** of the processing
- The **type of personal data** and **categories of data subjects**, and
- The obligations and rights of the controller

The agreement must also provide that the processor must:

- Only act on the controller's **documented** instructions (unless legally obliged to do otherwise)
- Impose **confidentiality obligations** on all **personnel** who process the relevant data

- Ensure the **security** of the personal data that it processes
- Abide by the rules regarding appointment of **sub-processors**
- Implement measures to assist the controller in complying with the rights of data subjects
- Assist the controller in:
    - Complying with its **data security obligations**
    - Complying with its **personal data breach** obligations (both to a supervisory authority and individual data subjects), and
    - Completing **Data Protection Impact Assessments** and **obtaining approvals from Supervisory Authorities** where required
- At the controller's election, either **return or destroy the personal data** at the end of the relationship (except as required by law), and
- Provide the controller with **all information necessary** to demonstrate compliance with the DPJL, which, in practice, means complying with an audit/inspection regime

TRANSFER

The DPJL (Article 67) provides that data controllers and processors may only transfer personal data out of the European Economic Area if one of the following conditions are met:

- The transfer is to a jurisdiction which has been held by the European Commission to provide an adequate level of protection for personal data (which would include a transfer to the United States to the extent that the data recipient participates in the Privacy Shield scheme)
- The transfer is made subject to 'appropriate safeguards' (Article 68 DPJL), which may include:
    - A legally binding and enforceable instrument between public authorities
    - Binding corporate rules approved by Jersey's Information Commissioner or another competent supervisory authority under the GDPR (or equivalent statutory provisions), or
    - Standard data protection clauses adopted by the Authority or by a competent supervisory authority and approved by the European Commission
- An exemption applies, the most commonly utilized of which are as follows:
    - The transfer is specifically required by a Jersey court
    - The data subject explicitly consents
    - The transfer is necessary for the performance of a contract to which the data subject is party or the implementation of pre-contractual measures taken at the data subject's request
    - The transfer is necessary to carry out a contract between the data controller and a third party if the contract serves the data subject's interests
    - The transfer:
        - Is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings)
        - Is necessary for the purpose of obtaining legal advice, or
        - Is otherwise necessary for the purposes of establishing, exercising or defending legal rights
    - The transfer protects the data subject's vital interests where:
        - The data subject is physically or legally incapable of giving consent
        - The data subject has unreasonably withheld consent, or
        - The controller or processor cannot reasonably be expected to obtain the explicit consent of the data subject

SECURITY

Controllers and processors must implement technical and organizational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data that are proportionate to the risk of harm posed to the rights of data subjects by such events (Article 21 DPJL).

'Technical measures' may include:

- The pseudonymization and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

BREACH NOTIFICATION

The DPJL includes obligations related to 'personal data breaches', which are defined in the DPJL as breaches of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data controllers must notify the Information Commissioner via an online portal (https://oicjersey.org/breach-reporting/) that a personal data breach has occurred within 72 hours of becoming aware of the breach (Article 20 DPJL). A breach does not need to be notified to the Information Commissioner where it is unlikely to result in a risk to the rights and freedoms of natural persons in respect of their personal data. If there is a high risk that the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the data controller must also notify those individuals.

Controllers are also required to keep a record of all data breaches (Article 20(5) DPJL) (whether or not notified to the Information Commissioner) and permit audits of the record by the Information Commissioner.

ENFORCEMENT

In Jersey, the Authority is responsible for the enforcement of the DPJL and DPAJL. Its day-to-day powers are delegated to the Information Commissioner, with the exception of the issuing of public statements and imposing fines.

The Authority has wide powers to require information and to enter and search premises (Schedule 1 DPAJL). It may also conduct and/or require an audit of a controller or processor.

The Information Commissioner may take the following enforcement actions:

Reprimand

The DPAJL does not specify the conditions upon which a reprimand may be issued; however most will likely take the form of a notice, and may be issued in combination with an administrative fine or a formal undertaking by the controller or processor to meet future compliance with any part of the DPJL or DPAJL.

Warning

This sanction applies where it appears to the Information Commissioner that the intended processing or other act or omission is likely to contravene the DPJL or DPAJL. Such warnings may be issued by way of a formal notice in advance of any intended processing.

Order

This refers to a formal notice of enforcement and can order any or all of the following:

- Bring specified processing operations into compliance with the DPAJL or DPJL, or take any other specified action required to comply with the same, in a manner and within a period specified in the order
- Notify a data subject of a personal data breach
- Comply with a request made by the data subject to exercise a data subject right
- Rectify or erase personal data
- Restrict or limit the recipient's processing operations, and
- Notify persons to whom the personal data has been disclosed of the rectification, erasure or temporary restriction on processing

Administrative Fines

The DPAJL also empowers the Authority to impose administrative fines (Article 26 DPAJL), which may be imposed in addition to any other sanctions.

An administrative fine must not exceed £300,000 or 10% of the person's total global annual turnover or total gross income in the preceding financial year, whichever is the higher (Article 27(2) DPAJL).

An administrative fine ordered against any person whose processing of data that gave rise to the fine was in the public interest and not for profit must not exceed £10,000 (Article 27(3) DPAJL).

Subject to the above limits, an administrative fine of up to £5 million may be ordered for:

- Failure to make reasonable efforts to verify that a person giving consent to the processing of the personal data of a child as required by Article 11(4) of the DPJL (information society services) is a person duly authorized to give consent to that processing
- Breach of Article 7 of the DPJL (obligations of joint controllers)
- Breach of Part 3 of the DPJL (which includes record-keeping obligations, data protection by design and default, data protection impact assessments, appointment conditions for data processors and breach notification)
- Breach of Part 4 of the DPJL (which includes information security obligations and general obligations on processors), and
- Breach of Part 5 of the DPJL (which includes obligations relating to data protection officers)

An administrative fine of up to £10 million may be imposed for:

- Breach of Part 2 of the DPJL (which includes fundamental duties of controllers, including compliance with the data protection principles, data subject information provisions and rules regarding consent) other than for Articles 7 and 11(4), and
- Breach of Part 6 of the DPJL (Data Subject Rights)

Right to claim compensation

The DPJL makes specific provision for individuals to bring private claims against controllers and processors.

Where a controller has breached the transparency and data subject rights provisions of the DPJL, a data subject may ask the Royal Court to make such order as it considers appropriate, which may include:

- An award of compensation for loss, damage or distress in respect of the violation
- An injunction (including an interim injunction) to restrain any actual or anticipated violation
- A declaration that the controller is responsible for the violation or that a particular act, omission or course of conduct on the part of the controller would result in a violation, and
- Requiring the controller to give effect to the transparency and data subject rights provisions (unless, in the case of a data subject access request, the Royal Court is satisfied that complying with the request will cause serious harm to a third party's physical or mental health)

Any person who has suffered "loss, damage or distress" as a result of a breach of the DPJL has the right to receive compensation (Article 69 DPJL) from the controller or processor. This means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss. In addition, data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 70). Individuals also enjoy the right to lodge a complaint with the Information Commissioner in relation to any violation of the DPJL that affects him or her (Article 19 DPAJL). Last, all natural and legal persons, including individuals, controllers and processors, have the right to complain to the Royal Court about a decision, or failure to make a decision, of the Authority or Information Commissioner concerning him or her.

Offenses

The DPJL contains the following offenses:

- Unlawfully obtaining personal data (Article 71 DPJL)
- Requiring a person to produce certain records (Article 72 DPJL)
- Providing false information (Article 73 DPJL), and
- Obstruction (Article 74 DPJL)

The DPAJL contains the following offenses:

- Failing to register with the Authority as a controller or processors (Art.17(6) DPAJL), and
- Failing to comply with an order made by the Authority following a breach determination (Article 25(8) DPAJL)

If a company or other organization commits a criminal offense under the DPJL or DPAJL, any partner, director, manager, secretary or similar officer or someone purporting to act in such capacity is personally guilty of an offense in addition to the corporate body if:

- The offense was committed with his or her consent or connivance, or
- The offense is attributable to any neglect on his or her part

ELECTRONIC MARKETING

The DPJL applies to most electronic marketing activities, as they involve some use of personal data *(eg,* an email address that includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller.

Where consent is relied upon, the strict standards for consent under the DPJL apply, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the checking of an unchecked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 36 DPJL).

ONLINE PRIVACY

Jersey has no specific law regulating online privacy; however, the DPJL and DPAJL generally apply.

KEY CONTACTS

Carey Olsen Jersey LLP
www.careyolsen.com

Huw Thomas
Counsel
Carey Olsen Jersey LLP
T +44 1534 888900
huw.thomas@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

KAZAKHSTAN

Last modified 28 January 2019

LAW

The main legal act regulating personal data in Kazakhstan is the law of the Republic of Kazakhstan No. 94-V dated May 21, 2013 'On Personal Data and Its Protection' (the 'Law').

There are also a number of other laws providing for personal data protection requirements, including:

- The Law on Informatisation
- The Law on Communication
- The Labour Code of Kazakhstan

DEFINITIONS

'**Personal data**' is any information relating to a specific individual (personal data subject) or a personal data subject who can be identified on the basis of such information which is recorded on electronic, paper and / or another tangible medium.

The law divides personal data into:

- '**Generally accessible personal data**', which is personal data that can be accessed freely with the consent of the personal data subject or to which confidentiality requirements do not apply in accordance with Kazakh law, and
- '**Limited access personal data**', which is personal data, access to which is limited by Kazakh law

Kazakh law does not provide an express definition of sensitive personal data. In certain cases, sensitive personal data may qualify as limited access personal data and, as such, it is additionally regulated by sector-specific laws of Kazakhstan (*eg,* medical secrecy, subscriber data).

NATIONAL DATA PROTECTION AUTHORITY

State regulation of personal data and its protection is carried out by various state authorities.

The government of Kazakhstan

- Develops the main directions of state policy
- Manages activities of central and local executive bodies
- Approves the procedure for determining by an owner and / or operator of a database containing personal data of the list of personal data that are necessary and sufficient for performing the owner's and / or operator's tasks
- Approves the procedure for implementation of measures for the protection of personal data by an owner and / or an operator of a database containing personal and a third party having access to such database, etc

State authorities, each within its competence

- Develop and / or approve regulatory acts
- Consider appeals of individuals and / or legal entities regarding personal data and protection of personal data issues
- Take measures for bringing persons who have violated personal data legislation of Kazakhstan to liability
- Exercise other powers provided for by Kazakh law

Prosecution authorities

- Carry out the highest supervision over observance of law in the field of personal data and its protection

REGISTRATION

Under Kazakh law, there is no express registration requirement in relation to personal data and its protection.

DATA PROTECTION OFFICERS

Under Kazakh law, an owner and / or operator of a database containing personal data and a third party having access to such database should, inter alia, when collecting and processing personal data, determine:

- A list of persons carrying out collection and processing of personal data or having access to it, and
- A list of persons responsible for compliance with data protection requirements.

COLLECTION & PROCESSING

Kazakh law requires those collecting and processing personal data to have the consent of the personal data subject or his / her legal representative. Such consent should be given in writing or in the form of an electronic document with the use of protective measures.

As a general rule, personal data subjects or their representatives may revoke their consent. However, the consent may not be revoked in cases where such revocation contradicts requirements of Kazakh law or there are any unfulfilled obligations.

Kazakh law allows the collection and processing of personal data without the consent of a personal data subject or his / her legal representative in cases explicitly prescribed by Kazakh law. Such cases may include, inter alia:

- Exercise of activities of law enforcement bodies and courts
- Implementation of state statistical activities
- Implementation of international treaties ratified by Kazakhstan
- Protection of constitutional rights and freedoms of a person, if obtaining the consent of a personal data subject or his / her legal representative is impossible
- Carrying out legal professional activities of a journalist, carrying out mass media, scientific, literary or other creative activities, subject to compliance with requirements of Kazakh law

Under Kazakh law, access to personal data is determined by the terms of consent for collection and processing of personal data, unless otherwise provided by Kazakh law. A person should be denied access to personal data if he / she refuses to assume obligations to ensure compliance with the requirements of the Law or may not ensure it.

Persons having access to limited access personal data should ensure its confidentiality.

Under Kazakh law, accumulation of personal data is carried out by collecting personal data that is necessary and sufficient to fulfill the tasks performed by an owner and / or an operator of a database containing personal data and by a third party having access to such database.

Personal data should be stored in databases located in Kazakhstan.

The period for retention of personal data is determined by the date of fulfillment of the purpose(s) for collection and processing of the personal data, unless otherwise provided by Kazakh law.

TRANSFER

Transfers of personal data are allowed if they do not violate the rights and freedoms of a personal data subject and do not affect the legitimate interests of other individuals and / or legal entities.

The transfer of personal data in cases that go beyond the previously stated purposes of its collection is permitted if carried out with the consent of a personal data subject or his / her legal representative.

The cross-border transfer of personal data to other countries is carried out only in cases where such countries ensure protection of personal data.

The cross-border transfer of personal data to countries that do not ensure protection of personal data is possible:

- With the consent of the personal data subject or his / her legal representative to the cross-border transfer of his / her personal data
- In cases stipulated by international treaties ratified by Kazakhstan
- In cases provided for by Kazakh law, if it is necessary for protecting the constitutional system, public order and public health and morals and rights and the freedoms of a person in Kazakhstan
- In case of protection of constitutional rights and freedoms of a person, if obtaining the consent of a personal data subject or his / her legal representative is impossible

Kazakh law may in certain cases prohibit the cross-border transfer of personal data.

SECURITY

Collection and processing of personal data is carried out only if its protection is ensured. Kazakh law defines protection of personal data as a set of legal, organization and technical measures.

The owner and / or operator of a database containing personal data and a third party having access to such database are required to take measures for protecting personal data, which ensure:

- Prevention of unauthorized access to personal data
- Timely detection of the facts relating to an incident of unauthorized access to personal data, if such unauthorized access could not be prevented
- Minimizing adverse effects of unauthorized access to personal data

The obligations of an owner and / or operator of a database containing personal data and a third party having access to such database to protect personal data arise from the moment of collecting the personal data and remain in force until such personal data is destroyed or depersonalized.

Kazakh law provides for additional requirements with regard to protection of electronic resources containing personal data.

BREACH NOTIFICATION

There is no express breach notification requirement under Kazakh law in relation to personal data and its protection. However, an owner and / or operator of a database containing personal data and a third party having access to such database may be required to notify personal data subjects or state authorities about a breach based on the general principles of Kazakh law.

There is no express mandatory breach notification requirement under Kazakh law in relation to personal data and it protection.

ENFORCEMENT

Generally, all state authorities of Kazakhstan, depending on their competences, (1) may consider appeals of individuals and / or legal entities regarding personal data and protection of personal data issues and (2) take measures against persons who have violated the personal data legislation of Kazakhstan.

The Prosecution Authorities of Kazakhstan supervise compliance with the personal data legislation of Kazakhstan and may also take measures against persons who have violated the personal data legislation of Kazakhstan. Interested persons may file complaints to the Prosecutor's Office regarding breaches of the legislation in relation to personal data and its protection.

Kazakh law provides for administrative and criminal liability for the violation of legislation in relation to personal data and its protection.

ELECTRONIC MARKETING

Kazakh law does not expressly regulate personal data and its protection in relation to electronic marketing. However, electronic marketing should be carried out in compliance with the law 'On Advertisement' and the law. As such, for example, the consent of a personal data subject should be obtained for the collection and processing of his / her personal data for electronic marketing purposes.

ONLINE PRIVACY

Kazakh law does not specifically regulate online privacy.

KEY CONTACTS

Dinara Jarmukhanova
Partner, Head of Kazakh practice
Centil Law Firm
T +7 727 315 0784
dinara.jarmukhanova@centil.law

Dariga Adanbekova
Associate
Centil Law Firm
T +7 727 315 0784
dariga.adanbekova@centil.law

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

KENYA

Last modified 28 January 2019

LAW

Kenya does not currently have a generally applicable data protection law. However, there are various legal sources that address data protection, including the Constitution of Kenya 2010, the Access to Information Act 2016 (applicable to public bodies), Health Act 2017 and the Computer Misuse and Cybercrimes Act 2018.

Currently, there are two draft data protection bills under consideration, which are separately undergoing legislative process and stakeholder consultation. As of now it is unclear whether one of these bills will ultimately be passed.

DEFINITIONS

Definition of personal data

The Access to Information Act 2016, which applies to public bodies, defines **personal information** as recorded information about an identifiable person, which includes information about the person's:

- Race
- Gender
- Sex
- Pregnancy
- Marital status
- National or ethnic origin
- Age
- Physical, psychological or mental health
- Well-being
- Disability
- Religion
- Conscience
- Belief
- Culture
- Language
- Birth
- Education
- Medical, criminal or employment history
- An identifying number, symbol or other identifiers assigned to that person
- Fingerprints, blood type or inheritable characteristics
- Opinion of a third party
- Contacts
- Personal correspondence with home or family

Definition of sensitive personal data

No specific definition at present.

NATIONAL DATA PROTECTION AUTHORITY

Kenya does not currently have a national data protection authority. However, there is draft legislation in the Senate, the Data Protection Bill 2018, that aims to establish such an authority.

REGISTRATION

Kenyan law does not currently require registration with a data protection authority or other governmental body.

DATA PROTECTION OFFICERS

Kenyan law does not currently require data protection officers to be appointed.

COLLECTION & PROCESSING

Kenyan law does not currently address collection and processing of personal data. However, the Health Act 2017 requires the Cabinet Secretary for Health to enact legislation that will regulate, among other things, collection and use of personal health information.

Draft regulations have not yet been issued.

Persons who collect and process personal data are currently only subject to contractual provisions regarding confidentiality, court orders and the common law duty of confidentiality.

TRANSFER

Transferors need to comply with the common law duty of confidentiality when transferring data to third parties, including outside of Kenya.

Further, the Computer Misuse and Cybercrime Act 2018 prohibits the transfer of an intimate or obscene image of another person. Violations of the prohibition are punishable by fines of up to KSh200,000 (US$2,000) and imprisonment of two years. However, currently, most of the provisions of the Computer Misuse and Cybercrime Act 2018 have been suspended by Kenyan courts, pending the conclusion of a case challenging the Act.

SECURITY

Kenyan law does not currently include any statutory security requirements. However, a holder of personal information may be subject to a contractual or a general obligation to ensure the technical and organizational safeguarding of such confidential information.

BREACH NOTIFICATION

Currently no requirement.

ENFORCEMENT

Currently, Kenyan courts are tasked with the enforcement of Kenya's limited data protection requirements.

ELECTRONIC MARKETING

Although Kenya's Consumer Protection Act 2012 seeks to protect consumers from unfair trade practices and the Kenya Information and Communications Act No. 2 of 1998 governs e-commerce transactions, no Kenyan laws specifically regulate

electronic marketing.

ONLINE PRIVACY

Kenyan law does not currently regulate online privacy.

KEY CONTACTS

Hassan Kibet
Associate
Iseme Kamau & Maema Advocates
T +254 722 898 393
hkibet@ikm.co.ke

Dennis Gathara
Associate
Iseme Kamau & Maema Advocates
T +254 722 898 393
dgathara@ikm.co.ke

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

KUWAIT

Last modified 28 January 2019

LAW

Kuwait does not have a specific personal data protection law. There are no clear legal guidelines to determine how and when personal data may be:

- Collected
- Stored
- Transferred
- Used, or
- Otherwise processed

Law No. 20 of 2014 (the E-Commerce Law) requires that client data relating to positional affairs, personal status, health status, certain financial information and other personal information must be retained privately and confidentially by the recipient and its employees. Such data may not be disclosed without client consent or a court order.

DEFINITIONS

Definition of personal data

Kuwaiti law does not define personal data. However, **personal data** is considered to include at least personal information about a person's:

- Positional affairs
- Personal status
- Health status, or
- Elements of financial disclosures

These elements are undefined, but broadly construed to encompass any personal information relating to the specified data element.

Definition of sensitive personal data

Kuwaiti law does not define sensitive personal data.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in Kuwait.

REGISTRATION

Not required.

DATA PROTECTION OFFICERS

Not required.

COLLECTION & PROCESSING

The E-Commerce Law includes a general obligation prohibiting Kuwaiti governmental bodies from collecting or processing any information in an illegal manner without the consent of the concerned person or his or her representative.

TRANSFER

The E-Commerce Law similarly includes a general obligation prohibiting Kuwaiti governmental bodies from transferring any information in an illegal manner without the consent of the concerned person or his or her representative.

SECURITY

No specific provisions.

BREACH NOTIFICATION

No specific provisions.

ENFORCEMENT

Violations of the E-Commerce Law are punishable by a maximum of three years imprisonment, and fines of no less than KWD5,000 (US$17,500) for anyone who discloses personal information without proper consent or a court order. The E-Commerce Law also provides for confiscation of tools, programs or devices used for unauthorized disclosure.

ELECTRONIC MARKETING

No specific provisions.

ONLINE PRIVACY

No specific provisions.

KEY CONTACTS

Kashif Syed
Senior Legal Consultant
DLA Piper
T +965 2291 5800
kashif.syed@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

KYRGYZSTAN

Last modified 21 January 2019

LAW

The Law of the Kyrgyz Republic on Personal Data No.58 dated 14 April 2008 ('The Law on Personal Data')

DEFINITIONS

The Law on Personal Data provides that information recorded on a material carrier relating to a particular person, which identifies a specific person or which could be used to identify a specific person, directly or indirectly, by reference to one or more factors related to biological, economic, cultural, civil or social identity shall qualify as '**personal data**'.

Personal data include:

- Biographical and identification data
- Personal characteristics
- Information on marital status
- Financial status
- Health data

There is no clear definition of Sensitive Personal Data. Under the provisions of the Law on Personal Data, all personal data is confidential. It should be noted that the Holder (Owner) of personal data (ie the data controller) and the data processor are obliged to ensure protection of personal data to prevent:

- Unauthorized access
- Blocking
- Transmission
- As well as its accidental or unauthorized destruction
- Alteration or loss
- Provide guarantees in respect of technical security measures and organizational measures regulating processing of personal data

However, confidentiality of personal data does not apply in cases of anonymisation or on request of the individual to which the personal data relates.

NATIONAL DATA PROTECTION AUTHORITY

No state authority has been yet appointed as the regulator in the field of data protection.

REGISTRATION

The Law on Personal Data obliges Holders (Owners) of Personal Data Arrays to register with the competent state authority,

however, to the best of our knowledge, none of Holders (Owners) of Personal Data Array has been registered to date, in particular, due to the fact that such regulator does not exist.

According to the Law on Personal Data within the registration procedure the following must be provided:

- Name and details of Holders (Owners) of Personal Data Arrays (ie data controller)
- Purposes and procedures of collection and processing of personal data
- Retention and terms of storage
- List of collected personal data
- Categories or groups of personal data bearers
- A source of collecting of personal data
- Procedure of notification of data subjects on collecting and possible transfer of personal data
- List of measures regarding the regime of confidentiality and safety of personal data
- Authorized person responsible for working with personal data
- Receiving party or category of receiving parties of personal data
- Proposed transfer of personal data outside of the Kyrgyz Republic

DATA PROTECTION OFFICERS

Under the Law on Personal Data, Holders (Owners) of personal data (ie the data controller) must indicate in its registration the name and contact details of the person that is responsible for the work with personal data. However, the Law on Personal Data does not contain any direct obligations to appoint a Data Protection Officer.

COLLECTION & PROCESSING

One of the basic principles of dealing with personal data is that personal data must be collected for accurately pre-defined, stated and legal purposes and must not be further processed in any manner incompatible with those purposes.

Processing of personal data is permitted in the following cases:

- The data subject has given its consent
- If it is necessary for public authorities, local authorities within their competence established by laws of the Kyrgyz Republic
- If it is necessary to achieve the legitimate interests of Holders (Owners)
- When implementation of these interests does not preclude the exercise of rights and freedoms of data subjects with regard to the processing of personal data
- When it is necessary to protect the interests of the data subject
- If personal data are processed solely for the purposes of journalism or for the purpose of artistic or literary works

TRANSFER

The Law on Personal Data allows transfer of personal data both within the country and abroad.

Transfer of personal data within the Kyrgyz Republic

- Data subject must be informed (in any form within a week)
- Personal data may be transferred without consent of the data subject in the following cases:
    - Extreme necessity in order to protect the interests of the data subject
    - Upon request of state authorities, local authorities, if the requested list of personal data fall under the competence of the requesting authority
    - Under any other case established by laws of the Kyrgyz Republic

Transfer of personal data outside the Kyrgyz Republic

- The cross-border transfer is carried out on the basis of an international treaty between the countries, under which the

receiving party must provide adequate protection of the personal data
- Consent of the data subject has been obtained, or
- Personal data may be transferred to the countries that do not provide the adequate level of protection on certain conditions:
    - With consent of the data subject
    - If the transfer is necessary to protect the data subject's interests, or
    - If personal data are contained in the Public Personal Data database

When transferring personal data to the global information network (internet, etc) the Holder of the personal data (ie the data controller) transferring such data, shall provide the necessary means of protection with regard to the confidentiality of the information being transferred.

SECURITY

When processing personal data the Holder (Owner) of personal data (data controller) and processor shall:

- Prevent access of unauthorized persons to the equipment used for personal data processing (access control)
- Prevent unauthorized reading, copying, modification or removal of data media (control of data media use)
- Prevent unauthorized recording of personal data and alteration or destruction of stored personal data (entry control) and enable backdated determination of when, by whom and which personal data have been altered
- Ensure security of data processing systems, designed to transfer personal data irrespective of the data involved (control of data transmission means)
- Ensure that each user of a data processing system has only has access to the personal data which it is authorized to process (controlled access)
- Enable backdated determination of when, by whom and which personal data have been entered into the data processing system (input control)
- Prevent unauthorized reading, copying, alteration and destruction of personal data during the transmission and transportation of personal data (transport control)
- Ensure the confidentiality of the information in the course of personal data processing

BREACH NOTIFICATION

If the Holder (Owner) of personal data (data controller) transfers the personal data without consent of the data subject to a third party they must inform the data subject within a week.

ENFORCEMENT

Although the Law on Personal Data has been adopted, there is no enforcement practice of its provisions in place so far since no responsible state authority has been appointed yet.

ELECTRONIC MARKETING

Sending of electronic communications for advertising is generally subject to prior express consent of the recipient.

ONLINE PRIVACY

The Law on Electrical and Postal Communication establishes that all databases of telecommunication operators must be confidential and that telecom operators are obliged to keep communication data confidential.

KEY CONTACTS

Begaliev Kerim
Partner
Centil Law Firm
T +996 312 919780
kerim.b@centil.law

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

LATVIA

Last modified 16 October 2018

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Personal Data Processing Law has been approved by the parliament and came into force on July 5, 2018. This law provides legal prerequisites for the implementation of the GDPR in Latvia and replaced the current Personal Data Protection Law.

DEFINITIONS

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal**

convictions and offences (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Personal Data Processing Law reproduces the definitions of Article 4 of GDPR, and generally uses the same terminology as the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

According to The Personal Data Processing Law the Data State Inspectorate (DSI) will become an independent institution, however, still supervised by the government.

In addition to the tasks provided by the GDPR, The Personal Data Processing Law provides for the DSI to perform the following tasks:

- Verifying the compliance of the processing of personal data with the requirements of regulatory enactments when the controller is prohibited by law from providing information to the data subject, after receiving a relevant application from the data subject
- Investigating administrative offenses
- Participating, in accordance with its competence, in the drafting of laws and policies, and giving an opinion on draft laws and policy planning documents prepared by other institutions
- Providing opinions on the compliance of the personal data processing systems created by state and local government institutions with the requirements of regulatory enactments
- Monitoring the circulation of information society services in relation to the personal data protection
- monitoring the operation of credit information offices
- Issuing a license to credit information offices

- Cooperating with the supervisory authorities of foreign personal data protection, information disclosure and access control, and the prohibition of sending commercial communications
- Providing the transferring of a data subject's request for information concerning themselves to Eurojust and Europol
- Representing Latvia in international organizations and activities in the field of data protection
- Carrying out studies, analyzing situations, making recommendations, opinions and informing the public about current issues in the areas of its competence
- Performing other tasks prescribed by regulatory enactments

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Given that the GDPR does not provide for the registration of processing personal data, registries and systems will no longer exist. Pre-recorded data will remain as archived information about past activities.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale, or
- Its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws

- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Personal Data Processing Law provides no derogation from the requirements of the GDPR regarding data protection officers. The Personal Data Processing Law provides the rules for examining an individual's knowledge in data protection and obtaining the status of data protection officer. The Personal Data Processing Law allows data controllers and processors to appoint as data protection officer any person who has the qualifications pursuant to the requirements of the GDPR.

As regards the certification procedure, the Personal Data Processing Law provides for a delegation to the Cabinet of Ministers to determine the application procedure, the content and procedure of the qualification examination, the amount of fees and payment procedures for organizing the qualification exam. However, the qualification examination is not mandatory as it was under the previous Personal Data Protection Law. According to the Personal Data Processing Law, the certification will be voluntary, and a data controller or processor may appoint as data protection officer any qualified person irrespective of certification.

The Personal Data Processing Law also provides for a transitional provision stating that the Cabinet of Ministers shall assess the usefulness of the qualification examination, and submit an appropriate assessment to the parliament on the utility of such examination by June 30, 2021.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous,*" and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to re-purpose personal data – *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose

- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (*ie,* opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Personal Data Processing Law contains provisions on specific treatment related to the exercise of other fundamental rights of the individual, providing derogations relating to the data processing for archiving purposes, scientific or historical research purposes, statistical purposes, and the processing of national classified data.

The Personal Data Processing Law provides specific rules and exceptions regarding the journalistic, academic, artistic and literary processing of personal data. When processing data for these purposes, it is necessary to assess the balance between the right to privacy and freedom of expression.

The Personal Data Processing Law also provides for specific rules regarding the processing of data in the official publication. It states that the data published in the official publication is deleted by the publisher on the basis of a decision

of the DSI or a decision confirming that such publication does not comply with the provisions of the GDPR.

The consent of a child for the use of information society services is deemed lawful where the child is at least 13 years old, meaning that Latvia has chosen the lowest threshold regarding the age of the child. Where the child is below the age of 13 years, such consent will be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
d. The transfer is necessary for important reasons of public interest
e. The transfer is necessary for the establishment, exercise or defense of legal claims
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
g. The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Personal Data Processing Law imposes a limitation period with respect to a data subject's rights to information on the recipients or categories of recipients to whom the data have been transferred: the data subject has the right to receive information about transfers within the last 2 years. The Personal Data Processing Law does not provide any other derogations or additional requirements to the GDPR regarding the transferring of the data.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

The Personal Data Processing Law does not provide any derogations or additional requirements to the GDPR regarding security.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Personal Data Processing Law does not provide any derogations or additional requirements to the GDPR regarding breach notification duties.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define undertaking and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of undertaking. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called look through liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- data subjects' rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered material or non-material damage as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of non-material damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against

a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Enforcing the decisions provided for in Article 58 of the GDPR in relation to the imposition of a legal obligation, DSI will apply the Administrative Procedure Law. The administrative penalties are not separately provided in the Personal Data Processing Law.

The Personal Data Processing Law imposes a limitation period of 5 years for civil claims on the reimbursement of losses caused by the violations of the GDPR.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg,* an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Personal Data Protection Law does not specifically address (electronic) marketing. However the use of personal data for marketing purposes falls within the scope of the law. The provisions on electronic marketing are also included in the Law on Information Society Services, which requires prior express consent of the person before using his or her contact information (*eg,* email address, phone number) for electronic marketing purposes. This is also stressed in the guidelines provided by DSI.

According to the provisions of the Law on Information Society Services no consent is required if the data has been obtained in the course of the sale of goods or provision of services, occurs for the same or similar goods or services, the recipient is able to decline easily and with no costs for the use of his or her personal data and the recipient has not previously declared that he or she does not want to be contacted.

With the Amendments of April 19, 2017, the Law on Information Society Services also contains procedures for submitting and reviewing complaints which states that the end user has the right to submit any complaints regarding the provision of the electronic communications services (thus also possibly any data protection issues), firstly, to the relevant electronic communications merchant and afterwards to the Public Utilities Commission.

The Personal Data Processing Law does not provide any derogations or additional requirements to the GDPR regarding electronic marketing.

ONLINE PRIVACY

Specific issues of online privacy are regulated in the Electronic Communications Law and the Law on Information Society Services.

The Law on Information Society Services states that the storage of information received, including cookies or similar technologies, is permitted, provided that the consent of the person has been received after he or she has received clear and comprehensive information regarding the purpose of intended storage and data processing. Therefore, with regard to cookies Latvian law supports an opt in approach.

As to location data, the Electronic Communications Law permits the processing of location data only to ensure the provision of electronic communications services or if the express prior consent is obtained. The person whose location data is being processed has the right to revoke his or her consent or to suspend it at any time, notifying the relevant electronic communications merchant of this revocation or requested suspension.

The processing of location data for other purposes without the consent of a user or subscriber is permitted only if it is not possible to identify the person utilizing such location data or if the processing of location data is necessary for emergency services.

The Personal Data Processing Law does not provide any derogations or additional requirements to the GDPR regarding online privacy.

KEY CONTACTS

Sorainen
www.sorainen.com/

Ieva Andersone
Senior Associate, Head of Commercial & Regulatory Practice Group in Latvia
T +371 67 365 000
ieva.andersone@sorainen.com

Andis Burkevics
Senior Associate
T +371 67 365 007
andis.burkevics@sorainen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

LESOTHO

Last modified 28 January 2019

LAW

The right to privacy is recognized and protected under the Constitution of the Kingdom of Lesotho.

Lesotho has established a Data Protection Act (the DP Act). The DP Act provides principles for the regulation of the processing of any personal information in order to protect and reconcile the fundamental and competing values of personal information privacy.

DEFINITIONS

Definition of personal data

The DP Act defines personal data or information as being information about an identifiable individual that is recorded in any form, including:

- Information relating to the race, national or ethnic origin, religion, age or marital status of the individual
- Information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved
- Any identifying number, symbol or other particular assigned to the individual
- The address, fingerprints or blood type of the individual
- The name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual
- Correspondence sent to a data controller by the individual that is explicitly or implicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence
- The views or opinions of any other person about the individual

Definition of sensitive personal data

The DP Act defines sensitive personal information as any of the following:

- Genetic data, data related to children, data related to offenses, criminal sentences or security measure, biometric data as well as, if they are processed for what they reveal, personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, affiliation, trade-union membership, gender and data concerning health or sex life
- Any personal information otherwise considered by Lesotho law as presenting a major risk to the rights and interests of

the data subject, in particular unlawful or arbitrary discrimination.

Section 29 prohibits a data controller from processing sensitive personal information, unless specifically permitted under the DP Act.

Section 36 contains general exemptions to the prohibition on processing sensitive personal information. These include instances where:

- Processing is carried out with prior parental consent where the data subject is a child and is subject to parental control in terms of the law
- The processing is necessary for the establishment, exercise or defense of a right or obligation in law
- Processing is necessary to comply with an obligation of international public law
- The Commission has granted authority in terms of section 37 for processing in the public interest, and appropriate guarantees have been put in place in law to protect the data subject's privacy
- Processing is carried out with the consent of the data subject
- The information has deliberately been made public by the data subject

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Commission (Commission).

Part 2 of the DP Act provides for the establishment of a Data Protection Commission, an independent and administrative authority established to have oversight and control over the DP Act and the respective rights of information privacy.

The powers and duties of the Commission are set out in section 8 of the DP Act.

REGISTRATION

The DP Act (section 25(5)) requires that a data controller process personal information only upon notification to the Commission.

DATA PROTECTION OFFICERS

The DP Act (section 58) authorizes the head of a data controller to designate, by order, one or more officers or employees to be Data Protection Officers of that controller. In terms of that order, the Data Protection Officers may exercise, discharge or perform any of the power, duties or functions of the head of the data controller under this Act.

COLLECTION & PROCESSING

The DP Act defines processing as an operation or activity or any set of operations, whether or not by automatic means relating to any of the following:

- The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use
- Dissemination by means of transmission, distribution or making available in any other form
- Merging, linking, as well as blocking, degradation, erasure, or destruction, of information

Under the DP Act (section 15(2)), personal information may only be processed where one of the following applies:

- The data subject provides explicit consent to the processing

- Processing is necessary for the conclusion or performance of a contract to which the data subject is a party
- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary to protect the legitimate interests of the data subject
- Processing is necessary for the proper performance of public law duty by a public body
- Processing is necessary for pursuing the legitimate interests of the data controller or of a third party to whom the information is supplied

Regarding the collection of data, the DP Act requires that a person shall collect personal information directly from the data subject, except where:

- The information is contained in a public record or has deliberately been made public by the data subject
- The data subject has consented to the collection of the information from another source
- Collection of the information from another source would not prejudice a legitimate interest of the data subject
- Collection of the information from another source is necessary:
    - To avoid prejudice to the maintenance or enforcement of the law and order
    - For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated
    - In the legitimate interests of national security
    - To maintain the legitimate interests of the data controller or of a third party to whom the information is supplied
- Compliance would prejudice a lawful purpose of the collection
- Compliance is not reasonably practicable in the circumstances of the particular case

TRANSFER

The DP Act distinguishes between the transfer of personal information to a recipient in a Member State of the South African Development Community (SADC) that has transposed the SADC data protection requirements and the transfer of personal information to a Member state that has not transposed the SADC data protection requirements or to a non-Member State.

Personal information shall only be transferred to recipients in a Member State that has transposed the SADC data protection requirements:

- Where the recipient establishes that the data is necessary for the performance of a task carried out in the public interest or pursuant to the lawful functions of a data controller, or
- Where the recipient establishes the necessity of having the data transferred and there is no reason to assume that the data subject's legitimate interests might be prejudiced by the transfer or the processing in the Member State

Further to the above, the DP Act requires that the controller make a provisional evaluation of the necessity for the transfer of the data. The recipient shall ensure that the necessity for the transfer of the data can be subsequently verified. The data controller shall ensure that the recipient shall process the personal information only for the purposes for which they were transferred.

Personal information may only be transferred to recipients, not SADC Member States subject to national law adopted pursuant to the SADC data protection requirements, if an adequate level of protection is ensured in the country of the recipient and the data is transferred solely to permit processing otherwise authorized to be undertaken by the controller.

The adequacy of the level of protection afforded by the relevant third country in question shall be assessed in the light of all the

circumstances surrounding the relevant data transfer(s), particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing, the recipient's country, the relevant laws in force in the third country and the professional rules and security measures which are complied with in that recipient's country.

SECURITY

N/A

BREACH NOTIFICATION

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an authorized person, the data controller, or any other third party processing personal information under the authority of a data controller, shall notify:

- The Commission, and
- The data subject, unless the identity of such data subject cannot be established

The notification shall be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the data controller's information system.

The data controller, in terms of section 23(3), shall delay notification to the data subject where the Lesotho Mounted Police Service, the National Security Service or the Commission determines that notification will impede a criminal investigation.

The breach notification to a data subject shall be in writing and communicated to the data subject in one of the following ways:

- Mailed to the data subject's last known physical or postal address
- Sent by email to the data subject's last known email address
- Placed in a prominent position on the website of the party responsible for notification
- Published in the news media
- As may be directed by the commission

The notification is required to provide sufficient information to allow the data subject to take protective measures against potential consequences of the compromise, including, if known to the data controller, the identity of the unauthorized person who may have accessed or acquired the personal information.

Mandatory breach notification

See above.

ENFORCEMENT

The Commission is responsible for the enforcement of the DP Act.

The DP Act also permits a data subject to institute a civil action for damages in a court having jurisdiction against a data controller for breach of any provision of this Act.

ELECTRONIC MARKETING

Direct marketing is defined in as a communication by whatever means of any advertising or marketing material which is directed to particular data subjects.

A data subject is entitled any time to require the data controller to cease, or not to begin, processing of personal data in respect of which he is the data subject for the purposes of direct marketing.

ONLINE PRIVACY

There are no sections of the DP Act which regulate privacy in relation to cookies and location data. These issues may be dealt with in future regulations, which the DP Act permits the Minister to make on the recommendations of the Commission.

KEY CONTACTS

Lungelo Magubane
Associate
DLA Piper
T +27 11 302 0819
lungelo.magubane@dlapiper.com

Savanna Stephens
Associate
T +27 11 302 0830
savanna.stephens@dlapiper.com

Monique Jefferson
Director
T +27 11 302 0853
monique.jefferson@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

LITHUANIA

Last modified 16 October 2018

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The implementation of the GDPR has been achieved in the Republic of Lithuania. The Law on Legal Protection of Personal Data (hereinafter 'Data Protection Law') has been in force since July 16, 2018.

The Data Protection Law replaced the Law on Legal Protection of Personal Data.

DEFINITIONS

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal**

convictions and offences (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Data Protection Law refers to the definitions provided by the GDPR. Only two definitions: 'direct marketing' and 'institutions and authorities are defined differently in the Data Protection Law.

Under the Data Protection Law, 'direct marketing' means any activity consisting of offering goods or services or asking opinion on the goods or services offered, by post, telephone or other direct means.

'Institutions and authorities' means state and municipal institutions and authorities, enterprises and public institutions, financed from state or municipal budgets and state monetary funds and authorized by the Law on Public Administration of the Republic of Lithuania to perform public administration activities or to provide public or administrative services to persons or to perform other public functions.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

In addition to the tasks established in the GDPR, the Data Protection Law authorizes the State Data Protection Inspectorate to perform the following tasks:

- To provide advice to data subjects, data controllers and processors on the protection of personal data and privacy protection, and also to develop methodological recommendations for the protection of personal data and to publish them publicly on their website
- To provide assistance to data subjects residing abroad on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)
- To cooperate with personal data protection supervisory authorities of other countries, European Union

institutions and international organizations and to take part in their activities
- To participate in the formation of state policy in the field of personal data protection and to implement it
- To implement the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)
- To perform other functions specified in the Data Protection Law and other legal acts

In addition to the powers established in the GDPR, the Data Protection Law authorizes the State Data Protection Inspectorate to:

- Receive all necessary information, copies of documents and duplicates, and copies of the data from the data controllers and data processors, state and municipal institutions and bodies, other legal and natural persons; as well as access to all data and documents which are necessary for the execution of tasks and functions of the State Data Protection Inspectorate
- During the investigation of the infringements to enter the premises of the person or entity which is subject to the inspection and to exercise similar actions with respect to related persons or entities
- Participate in meetings of the Parliament, the Government, and other state institutions when issues related to the protection of personal data or privacy are being considered
- Invite experts and consultants, to form working groups on examination of processing or protection of personal data, preparation of personal data protection documents and to deal with other issues which fall under the competence of the State Data Protection Inspectorate
- Provide recommendations and instructions to data controllers, data processors and other legal or natural persons regarding the processing of personal data or the protection of privacy
- Exchange information with other countries' personal data protection supervisory authorities and international organizations to the extent necessary for their functions
- Participate in court hearings when infringements of international, European Union or national law provisions on personal data protection issues are being considered
- Use technical measures during the investigation of infringements
- Receive oral and written explanations from legal entities and natural persons during the infringement proceedings and to demand that they arrive to provide explanations to the premises of the State Data Protection Inspectorate
- Use the information held by the State Data Protection Inspectorate, including personal data obtained during the investigation of infringements or received by the State Data Protection Inspectorate for other functions
- Involve police officers in order to ensure the possible use of violence and in order to maintain public order
- Perform other functions specified in the law

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Given that the GDPR does not provide for the registration of data processing activities, registries and related systems will no longer exist.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Data Protection Law does not determine any derogations from the requirements which are set in the GDPR regarding data protection officers.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous,*" and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an

official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to re-purpose personal data – *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two

months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate compelling legitimate grounds for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (*ie,* opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Data Protection Law contains provisions on specific conditions related to the processing of national identification number.

Article 3 of the Data Protection Law determines particularities of the processing of the personal code:

- Personal code can be processed if there is at least one of the conditions for the lawfulness of the processing of personal data referred to in Article 6(1) of Regulation (EU) 2016/679
- It is forbidden to disseminate the personal code
- It is forbidden to process personal code for direct marketing purposes

The Data Protection Law provides specific rules and exceptions regarding processing of personal data for journalistic, academic, artistic and literary purposes. When processing data for these purposes, Articles 12-23, 25, 30, 33-39, 41-50 and 88-91 of the GDPR shall not be applicable.

The Data Protection Law also provides specific rules regarding processing of personal data in the employment context:

- It is forbidden to process the personal data of candidates and employees related to convictions and offences committed by the candidate or employee, unless such personal data are necessary to verify that a person meets the requirements of law or implementing legislation for the purpose of performing work or other duties.
- The data controller may collect personal data relating to qualifications, professional skills and business characteristics of a candidate applying for job from a former employer by duly informing the candidate, and from the existing employer by receiving consent of the candidate.
- The processing of video or audio data in the workplace and at the data controller's premises or in the areas where employees work, in the processing of personal data relating to the monitoring of employees' behavior, employees must be informed of such processing of their personal data in writing or by any other means which allow to prove the fact that the information referred to in Article 13(1) and (2) of Regulation (EU) 2016/679 has been provided.

The consent of a child for the use of information society services is deemed lawful where the child is at least 14 years old. Where the child is below the age of 14 years, such consent will be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility for the child.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained;
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;

d. The transfer is necessary for important reasons of public interest;
e. The transfer is necessary for the establishment, exercise or defense of legal claims;
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Data Protection Law provides that the State Data Protection Inspectorate must issue an authorization for the transfer of personal data to a third country or an international organization in order for the transfer to be lawful. A substantiated written refusal to issue it within a maximum of 20 working days may also be communicated by the State Data Protection Inspectorate.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However, the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

The Data Protection Law does not provide any derogations or additional requirements to the GDPR regarding security.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Data Protection Law does not provide any derogations or additional requirements to the GDPR regarding breach notification duties.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent;
- Data subjects' rights;
- International transfer restrictions;
- Any obligations imposed by Member State law for special cases such as processing employee data; and
- Certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations;
- Obligations of certification bodies; and

- Obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The Data Protection Law sets out administrative fines which can be imposed on public institutions. The State Data Protection Inspectorate has the right to impose an administrative fine:

- Up to 0.5% of the annual budget of the institution in the current year or of the total annual revenue received in the previous year but not exceeding EUR 30000 for breach of the provisions referred to in the paragraphs a-c of Article 83(4) of the GDPR
- Up to 1% of the annual budget of the institution in the current year or of the total annual revenue received in the previous year, but not exceeding EUR 60000, for breach of the provisions referred to in the paragraphs a-e of Article 83(5) and Article 83(6) of the GDPR
- When a public authority or body carries on commercial business, according to sections 4-6 of Article 83 of the GDPR

The statute of limitation is two years from when the offence has been committed, and in case of continued offences, within two years after the offence has been identified.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Electronic marketing to individuals in Lithuania must only be conducted in accordance with the Data Protection Law, the Electronic Communications Law and the Law on Advertising of the Republic of Lithuania (Advertising Law). Only direct marketing tailored to natural persons is subject to the requirements of the above mentioned laws. Direct marketing actions that are targeting legal persons (*ie,* companies) are not subject to any of these regulations.

General requirements for direct marketing:

- The customer has given his prior consent (under Lithuanian law, an opt-in principle applies, *ie,* the customer should actively express his willingness to receive commercial communication)
- The customer consent must be obtained separately from other terms of the contract between the parties
- Consent cannot be obtained in the standard terms presented to the customer (*eg,* "by accepting these terms you agree to receive our commercial communication to the email provided to us"). The consent must stand separately from other contractual terms, so that the data subject has an actual possibility to choose whether he or she wants to receive commercial communication from the company or not
- The company must ensure that customers have been given a clear, free-of-charge and easily realizable possibility not to give their consent or refuse giving their consent for the use of this data for the above-mentioned purposes at the time of collection of the data and, if initially the customer has not objected against such use of the data, at the time of each offer

No direct marketing should be carried out where the contact has requested not to receive unsolicited direct marketing.

Exemption: if the company has legitimately obtained a telephone number from a customer within the scope of its business transactions, the company is permitted to use the telephone number for promotional communication if such communication is regarding similar goods or services of the service provider.

Additional requirements under the Advertising Law:

- Direct marketing must be clearly recognizable as a commercial communication
- The person on behalf of whom this commercial communication is distributed must be clearly identified
- The content of the offer and conditions regarding receiving of the service must be formulated clearly and precisely

Each marketing communication is a separate violation, for which a penalty of up to EUR 3,000 may be imposed.

As mentioned above, the Data Protection Law provides a definition of direct marketing and prohibits the processing of personal code for direct marketing purposes.

ONLINE PRIVACY

Traffic Data

Traffic Data held by a public electronic communications services provider must be erased or anonymized when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- It is being used to provide a value added service
- consent has been given for the retention of the Traffic Data

- It is required for investigation of a grave crime

Traffic Data can only be processed by a CSP for:

- The management of business needs, such as billing or traffic
- Dealing with customer enquiries
- The prevention of fraud
- The provision of a value added service

Cookies

The use of cookies is permitted only if approved by the user (under Lithuanian law, an opt-in principle applies). However, consent is not required for cookies used for website technical structure and for cookies used for showing website content. Consent is not required for session ID cookies and for so called 'shopping basket' cookies (these exceptions do not apply if such cookies are used for collecting statistical information on use of the website).

Clear and exhaustive information on use of cookies, including information about the purpose of cookie related data processing, must be provided. This information should be provided in the privacy policy of the website. Consent to the terms of the website's privacy policy or terms of use containing the information on use of cookies is considered insufficient. Consent though web browser settings may be considered adequate only if the browser settings allow choosing what cookies may be used and for what purposes. However, considering the nature of currently used web browsers consent through web browser settings is not considered appropriate under Lithuanian law.

Location data

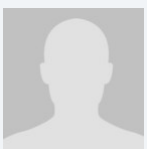
Processing of location data triggers personal data processing laws. The data controller must have a legitimate basis for such personal data processing (*eg*, the data subject has given his consent; a contract to which the data subject is party is being concluded or performed; it is a legal obligation of the data controller under laws to process personal data; processing is necessary in order to protect vital interests of the data subject; etc.).

The Data Protection Law does not provide any derogations or additional requirements to the GDPR regarding online privacy.

KEY CONTACTS

Sorainen
www.sorainen.com/

Kaupo Lepasepp
Partner
T +372 6 400 900
kaupo.lepasepp@sorainen.com



Mihkel Miidla
Partner, Head of Technology & Data Protection
T +372 6 400 959
mihkel.miidla@sorainen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

LUXEMBOURG

Last modified 10 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

Two Luxembourg Data Protection Laws of August 1, 2018 have been enacted to implement the GDPR:

- The Law on the organization of the National Data Protection Commission (CNPD) and the general data protection framework. It has repealed the previous Law on Data Protection (amended Law of August 2, 2002) and completes the GDPR at the national level. Most of all it gives the framework for the CNPD's organization, composition and powers under the GDPR and the applicable national law
- The Law on the protection of individuals with regard to the processing of personal data in criminal matters as well as in matters of national security

Article L. 261-1(1) of the Labor Code provides specific regulations concerning employer workplace surveillance.

In addition, the amended Law of May 30, 2005 on data protection and electronic communications governs the protection of personal data in the field of telecommunications and electronic communications, implementing the Directive 2002/58/EC.

DEFINITIONS

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definition of personal data has not been amended by applicable law. GDPR definitions apply.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Commission Nationale pour la Protection des Données (CNPD), 1, Avenue du Rock'n'Roll, L-4361 Esch-sur-Alzette, T +352 26 10 60 1; F +352 26 10 60 29.

The CNPD is in charge of monitoring and checking that the data are processed in accordance with the GDPR, as well as the Law of August 1, 2018 on the organization of the National Data Protection Commission, the Law of August 1, 2018 on the protection of individuals with regard to the processing of personal data in criminal matters and in matters of national security, and any applicable legislation that may include specific personal data protection provisions.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

No specific provisions in the applicable law.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

Article 65(1) of the Law of August 1, 2018 on the organization of the National Data Protection Commission provides for

a specific obligation to appoint a DPO in the context of processing of personal data for scientific or historical research purposes or statistical purposes. Such appointment must be made in accordance with the nature, scope, context and purposes of the processing, as well as the risks for the rights and freedoms of the relevant data subjects. In this regard, if the data controller elects not to appoint a DPO, it must then formally document and justify why it chose not to appoint a DPO, for each project involving a processing of personal data for scientific or historical research purposes or statistical purposes.

Article 64 of the Law of August 1, 2018 on the organization of the National Data Protection Commission provides that the same applies to processing of special categories of personal data for the purposes defined in Article 9(2)(j) GDPR (*ie,* processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes).

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous,*" and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to re-purpose personal data – *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (*ie,* opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Law of August 1, 2018 on the organization of the National Data Protection Commission provides specific regulations concerning the processing of personal data for the purposes of the surveillance of employees at the workplace by the employer (thus modifying Article L. 261-1(1) of the Labor Code). In this respect, the employer must comply with a certain set of obligations, in addition to its general obligations as a data controller under the GDPR.

Notably, the employer must inform certain employee representation bodies of the contemplated processing of personal data. This information must contain a detailed description of the purposes of the contemplated processing, the means of implementation of the surveillance, and the retention policy for the personal data concerned.

When employees or their representation bodies are informed that their personal data may be processed for surveillance purposes, they may ask the CNPD for a preliminary opinion on the compliance of such surveillance project with applicable data protection legislation. The employer may not begin surveillance until the CNPD hands out its decision.

When surveillance has already been put it place by the employer, employees have a right to file a complaint with the CNPD if they believe that processing does not comply with applicable data protection legislation. Filing such complaint may not be held as a grounds for dismissal.

Finally, the Law of August, 1 2018 on the organization of the National Data Protection Commission provides three specific provisions complementing the GDPR in matters left to Member State discretion.

1. **Processing of personal data for the sole purpose of journalism, university research, art or literature**

This processing is not subject to:

- Prohibitions on processing special categories of personal data set out under Article 9(1) GDPR
- Limitations applicable to processing of personal data relating to criminal convictions and offences (Article 10, GDPR):
    - Provided such processing concerns data made publicly available (in an obvious fashion) by the data subject

- If the data are directly connected to the public life of the data subject
- If the data are directly connected to an event in which the data subject has willingly become involved

- Obligations imposed on the data controller in case of a transfer of personal data to third countries or international organizations (Chapter V, GDPR)
- The obligation of the data controller to provide information to the data subject where personal data are collected from the data subject (Article 13, GDPR), when providing such information would jeopardize the collection of personal data from such data subject
- The obligation of the data controller to provide information to the data subject where personal data have not been obtained from the data subject (Article 14, GDPR), when providing such information would jeopardize either the collection of personal data, a publication project, making such personal data available to the public in any way whatsoever or would provide indications as to the source of information
- The obligation to provide the data subject with the right of access to his or her personal data. Such right is postponed and limited, in that it cannot enable the data subject to identify the source of information. This right may be exercised only through the CNPD and in the presence of the President of the Press Council or his or her representative

1. **Processing of personal data for scientific or historical research purposes, for statistical purposes, or for archiving purposes in the public interest**

When personal data is processed for scientific or historical research purposes or for statistical purposes, the rights of the data subject specified under articles 15, 16, 18 and 21 GDPR may be limited provided that such rights would make impossible or seriously impede the accomplishment of the specific concerned purposes.

Such limitation on data subject rights may only be applied where the data controller puts in place an extensive set of additional appropriate safeguard measures for the rights and freedom of the data subject (Article 65 of the Law of August 1, 2018 on the organization of the National Data Protection Commission), such as, in particular:

- The appointment of a DPO
- Performing an impact assessment of the contemplated processing on the protection of personal data
- Anonymizing the data processed

In any event, the additional safeguard measures must be put in place in accordance with the nature, scope, context and purposes of the processing, as well as the risks for the rights and freedoms of the relevant data subjects. In this regard, if the data controller elects not to put in place one of the measures listed in Article 65 of the Law of August 1, 2018 on the organization of the National Data Protection Commission, it must then formally document and justify why it chose not to do so.

Finally, processing of special categories of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 9(2)(j), GDPR) is allowed under the same conditions (*ie,* putting in place additional appropriate safeguard measures as defined under Article 65 of the Law of August 1, 2018 on the organization of the National Data Protection Commission).

1. **Processing of special categories of personal data**

Genetic data may not be processed for purposes of exercising the controller's own rights in the field of employment and insurance law.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)).

Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes, among others, binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
d. The transfer is necessary for important reasons of public interest
e. The transfer is necessary for the establishment, exercise or defense of legal claims
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
g. The transfer is made from a register, which according to EU or Member State law, is intended to provide information to the public, subject to certain conditions

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State (transfers in response to such requests where there is no other legal basis for transfer will infringe the GDPR).

No specific provisions in the applicable local law.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However, the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

Article 65 of the Law of August 1, 2018 on the organization of the National Data Protection Commission provides specific technical measures that must be put in place for limited categories of processing (*ie,* processing of personal data for scientific or historical research purposes or for statistical purposes, and processing of special categories of personal data for archiving purposes in the public interest).

Such measures include:

- Resorting to an independent trusted third party for the anonymization or pseudonymization of the personal data
- Log files allowing for the identification of the purpose, date and time of consultation of the personal data as well as for the identification of the person having collected, modified or deleted the personal data

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

No specific provisions in the applicable local law.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent

for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- Data subjects' rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The CNPD may:

- Impose administrative fines as provided for in Article 83 of the GDPR (however, it cannot impose such sanctions with respect to the State or municipalities)
- Impose on the controller or processor a penalty of up to five per cent (5%) of its average daily turnover in the previous financial year, respectively during the last financial year closed, as long as such controller or processor does not communicate an information requested by the CNPD pursuant to Article 58(1)(a) GDPR, or as long as

such controller or processor does not abide by a corrective measure adopted by the CNPD pursuant to Article 58(2)(c)-(j) GDPR
- Impose sanctions (an imprisonment of 8 days or a fine of between EUR 251 and EUR 125,000) against anyone who knowingly prevents or hinders the performance of the CNPD's missions
- Order the insertion in full or by extracts of its decisions in newspapers or otherwise, at the expense of the person sanctioned

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg,* an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing is permissible only in respect of subscribers who have given their prior consent.

Where a supplier obtains from its customers their electronic contact details for electronic mail, in the context of the sale of products or services, that supplier may use those electronic contact details for direct marketing of its own similar products or services provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use.

The transmission of unsolicited communications for purposes of direct marketing by means other than those referred to in the previous paragraphs shall be permissible only with the prior consent of the subscriber concerned.

No specific provisions in the applicable local law.

ONLINE PRIVACY

Traffic Data

For the purposes of the investigation, detection and prosecution of criminal offences, and solely with a view to enabling information to be made available, in so far as may be necessary, to the judicial authorities, any service provider or operator processing traffic data must retain such data for a period of six months. This obligation includes data related to the missed phone calls wherever these data are generated, stored or recorded. Beyond this period, the service provider or operator must erase such data unless made anonymous.

Traffic data may be processed for the purposes of marketing electronic communications services or providing value added

services, to the extent and for the duration necessary for such supply or marketing of such services, provided that the provider of an electronic communications service or the operator has informed the subscriber or user concerned in advance of the types of traffic data processed and of the purpose and duration of the processing, and provided that the subscriber or user has given his or her consent, notwithstanding his or her right to object to such processing at any time.

Location Data other than Traffic Data

Service providers or operators have also the obligation to retain location data other than traffic data for a period of six months for the purposes of the investigation, detection and prosecution of criminal offences. This obligation includes data related to missed phone calls wherever these data are generated, stored or recorded. Beyond this period, the service provider or operator must erase such data unless made anonymous.

Service providers or operators may process location data other than traffic data relating to subscribers and users only if such data have been made anonymous or the subscriber or user concerned has given his or her consent, to the extent and for the duration necessary for the supply of a value added service.

Service providers and, where appropriate, operators shall inform subscribers or users in advance of the types of location data other than traffic data processed, of the purposes and duration of the processing and whether the data will be transmitted to third parties for the purpose of providing the value added service. Subscribers or users shall be given the possibility to withdraw their consent to the processing of location data other than traffic data at any time.

Where subscriber or user consent has been obtained for the processing of location data other than traffic data, the subscriber or user must continue to have the possibility, using a simple means free of charge, to temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication.

Cookies

Prior informed consent of a subscriber or user is required. The method of providing information and the right to refuse should be as user friendly as possible and, where it is technically possible and effective, the users consent may be expressed by appropriate browser or application settings.

No specific provisions in the applicable local law.

KEY CONTACTS

Olivier Reisch
Partner
T +352 26 29 04 2017
olivier.reisch@dlapiper.com

Eugene H.C. Tchen
Of Counsel
T +352 26 29 04 25 69
eugene.tchen@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MACAU

Last modified 28 January 2019

LAW

Macau personal data protection Law no. 8/2005 of August 22nd (Law).

DEFINITIONS

Definition of personal data

The Law defines personal data as any information of any type, in any format, including sound and image, related to a specific or identifiable natural person (data subject). An 'identifiable natural person' is anyone who can be identified, directly or indirectly, in particular by reference to a specific number or to one or more specific elements related to his or her physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

The Law defines sensitive personal data as any personal data revealing political persuasion or philosophical beliefs, political and joint trade union affiliation, religion, private life, racial or ethnical origin or data related to health or sex life, including genetic data.

NATIONAL DATA PROTECTION AUTHORITY

The Office for Personal Data Protection (OPDP) is the Macau regulatory authority responsible for supervising and coordinating the implementation of the Law. https://www.gpdp.gov.mo/

REGISTRATION

The OPDP must be notified of any processing of personal data by a data processor unless an exemption applies.

For certain data categories *(eg,* certain sensitive personal data, data regarding illicit activities or criminal and administrative offenses or credit and solvency data) and certain specific personal data processing, data processors must obtain prior authorization from the OPDP.

The OPDP provides (official) forms that must be submitted regarding personal data processing, either in Portuguese or Chinese language, along with the following information (if applicable):

- Identification and contact details of the data processor and its representatives
- The personal data processing purpose
- Identification and contact details of any third party carrying out the personal data processing
- The commencement date of the personal data processing
- The categories of personal data processed (disclosing whether sensitive personal data, data concerning the suspicion of illicit activities, criminal and / or administrative offenses or data regarding credit and solvency are to be collected)

- The legal basis for processing personal data
- The means and forms available to the data subject for updating his or her personal data
- Any transfer of personal data outside Macau, along with the grounds for, and measures to be adopted with, the transfer
- Personal data storage time limits
- Interconnection of personal data with third parties
- Security measures adopted to protect the personal data

DATA PROTECTION OFFICERS

There is no legal requirement to appoint a data protection officer in Macau.

COLLECTION & PROCESSING

Personal data may be processed only if the data subject has given his or her unequivocal consent or if processing is deemed necessary:

- Execution of an agreement where the data subject is a party, or, at the data subject's request, negotiation in relation to such an agreement
- Compliance with a legal obligation to which the data processor is subject
- Protection of vital interests of the data subject if he or she is physically or legally unable to give his or her consent
- Performance of a public interest assignment or exercise of public authority powers vested in the data processor or in a third party to whom the personal data is disclosed, or
- Pursuing a data processor's legitimate interest (or the legitimate interest of a third party to whom the data is disclosed), provided that the data subject's interests or rights, liberties and guarantees do not prevail

The data subject must be provided with all relevant processing information, including the identification of the data processor, the purpose of processing, and the means and forms available to the data subject for accessing, amending and deleting his or her personal data.

TRANSFER

The transfer of personal data outside Macau can only take place if the recipient country ensures an adequate level of personal data protection, unless the data subject has provided clear consent and the required filings have been made with the OPDP.

SECURITY

The data processor must implement adequate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular, where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Such measures must ensure a security level appropriate to the risks represented by the personal data processing and the nature of the personal data, taking into consideration the state of the art and costs of the measures.

BREACH NOTIFICATION

None. The Law does not require data processors to notify either the OPDP or data subjects about any personal data breach.

ENFORCEMENT

Violations of the Law are subject to civil liability and administrative and criminal sanctions, including fines and / or imprisonment.

ELECTRONIC MARKETING

Under the Law, data subjects have the right to object, on their request and free of charge, to the processing of their personal data for direct marketing purposes, to be informed before their personal data is disclosed or used by third parties for the purpose of direct marketing and to be expressly offered, also free of charge, the right to object to such disclosure or use.

ONLINE PRIVACY

The Law also applies in the online environment.

For example, a Macau company that collects personal data from Macau residents through its website *(eg,* through cookies) must fulfil all obligations under the Law imposed on data processors. In particular, the Macau company must inform data subjects of the personal data processing purpose and notify the OPDP about the personal data processing.

KEY CONTACTS

LVT Lawyers
www.lvt-lawyers.com

Tang Weng Hang
Partner
T +853 2871 5588
tangwenghang@lvt-lawyers.com

António Lobo Vilela
Partner
T +853 2871 5588
lobovilela@lvt-lawyers.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MADAGASCAR

Last modified 25 January 2017

LAW

Law No. 2014-038 relating to protection of personal data is the main regulatory framework in Madagascar (the 'Data Protection Law').

After discussion at the National Assembly of Madagascar, the Data Protection Law was adopted on 16 December 2014. The Law was promulgated by the President of Republic of Madagascar on 9 January 2015.

In order to come into effect, the Data Protection Law must be published in the Official Gazette of the Republic of Madagascar. This is expected to occur during the course of this year.

DEFINITIONS

Definition of personal data

Personal data is any information relating to a natural person, whereby that person is or can be identified, directly or indirectly, by reference to a name, an identification number or to one or more elements specific to him/her such relating to physical, physiological, psychical, economic, cultural or social.

Definition of sensitive personal data

Sensitive personal data means data which includes information relating to:

- racial origin
- biometric and genetic information
- political opinion
- religious belief or others convictions
- trade-union affiliation
- health or sexual life.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Law provides for the creation of the C*ommission Malagasy sur l'Informatique et des Libertés* ('CMIL'). However, the CMIL has not yet been established.

REGISTRATION

Except for certain data processing that is subject to exemption, authorisation, ministerial order or decree, the processing of personal data requires a prior declaration to the CMIL.

The prior declaration to the CMIL shall specify, where relevant, inter alia:

- the identity and the address of the data controller (*responsable du traitement*) (ie the natural or legal person who either alone or jointly with other persons determines the purpose and the means of the personal data processing and implements such processing itself or appoints a data processor for that purpose)
- the purpose(s) of the processing
- the interconnections between databases
- the types of personal data processed, their origins and the categories of persons affected by the processing
- the duration for which the data will be kept
- the department or persons in charge of implementing the data processing
- the existence of data transfer to other country
- the measures taken in order to ensure the security of the processing
- the use of a data processor (*sous-traitant*).

The CMIL has to issue its decision on any authorisation application 2 months following receipt of the application. An additional time period of 2 months can be added to this period after decision of the President of the CMIL. The absence of decision of the CMIL during these periods is considered as a refusal of the application.

DATA PROTECTION OFFICERS

The Data Protection Law does not provide any legal requirement to appoint a data protection officer (*délégué à la protection des données à caractère personnel)* in Madagascar.

However, an entity is exempt from making prior *declarations* to the CMIL if the entity has appointed a data protection officer ('DPO').

The appointment of a DPO does not exempt an entity from requesting prior *authorisation*, where necessary (for example where there is a transfer of data to a country that does not provide an adequate level of protection for personal data).

The DPO must be a resident of Madagascar.

COLLECTION & PROCESSING

The following principles must be satisfied when personal data is collected and processed:

- all personal data must be processed fairly and lawfully for specific, explicit and legitimate purposes and subsequently processed in accordance with these purposes
- all personal data collected must be adequate, relevant and non-excessive in view of the purposes for which it is collected
- all personal data must be accurate and comprehensive and when necessary, kept up to date
- all personal data must be retained no longer than is necessary for the purposes for which it is processed.

The processing of personal data must receive the data subject's prior consent or fulfill one of the following conditions:

- compliance with a legal obligation of the data controller
- the purpose of the processing is to protect the individual's life

- the purpose of the processing is to carry out a public service
- the processing relates to the performance of a contract to which the concerned individual is a party, or pre-contractual measures requested by that individual
- processing relates to the realisation of the legitimate interest of the data controller or the data recipient, subject to the interest and fundamental rights and liberties of the concerned individual.

The conditions for processing of sensitive personal data include most of the above conditions, but contain an additional list of more restrictive conditions that must also be satisfied such as requirement to obtain prior consent of the data subject, or in the absence of consent where the processing is undertaken to carry out a public service and is required by law or priorly authorised by the CMIL.

TRANSFER

The transfer of a data subject's personal data to a third party country is allowed only if the country guarantees to individuals a sufficient level of protection in terms of privacy and fundamental rights and liberties.

The sufficiency of the protection is assessed by considering all the circumstances surrounding the transfer, in particular the nature of the data, the purpose and the duration of the proposed processing, country of origin and country of final destination, rules of law, both general and sectorial in force in the country in question and any relevant codes of conduct or other rules and security measures which are complied with in that country.

Data controllers may transfer personal data to a third country that is not deemed to offer adequate protection only if:

- the data subject consents and duly informed of the absence of adequate protection
- the transfer is necessary:
    - for the performance of a contract between the data controller and the individual, or pre-contractual measures undertaken at the individual's request
    - for the conclusion or the performance of a contract in the interest of the individual, between the data controller and a third party
    - for the protection of the public interest
    - for consultation of a public register intended for the public's information
    - to comply with obligations allowing the acknowledgment, the exercise or the defence of a legal right.

In all cases, the data recipient in the third party country cannot transfer personal data to another country, except with the authorisation of the first data controller and the CMIL .

SECURITY

The data controller must take all useful precautions, with respect to the nature of the data and the risk presented by the processing, to preserve the security of the data and, amongst other things, prevent alteration, corruption or access by unauthorised third parties.

BREACH NOTIFICATION

The Data Protection Law does not set out any general or specific obligation to notify the CMIL or the data subject in the event of a data security breach.

ENFORCEMENT

The CMIL has the power to proceed with verifications of any data processing, and, as the case may be, to request a copy of every document that it considers useful in respect of verifications. The CMIL agents are authorised to carry out online inspections and on-site verifications of a data controller or a data processor.

In cases where the CMIL is of the opinion that a data controller or a data processor has contravened the provisions of the Data Protection Law, then it may serve, in accordance with the severity of the violation committed:

- warnings and notices to comply with the obligations defined in the Data Protection Law
- notice of withdrawal of the authorisation
- a financial sanction of up to 5% of the last financial year pre-tax turnover (not deducted from tax turnover).

The Data Protection Law provides that any processing of personal data in contravention with its provisions is considered an offence. For example, processing of personal data without prior declaration to or authorisation of the CMIL can result in imprisonment of 6 months to 2 years (Article 62 of the Data Protection Law).

In addition to any penalty, the Court may order the erasure of all or part of the personal data which was the object of the processing considered an offence.

ELECTRONIC MARKETING

The Data Protection Law does not provide specific restrictions on the use of electronic marketing. However, the data subject has a right to opt out of allowing their personal data to be used for marketing purposes without providing any reason.

ONLINE PRIVACY

The Data Protection Law does not yet address location data, cookies, local storage objects or other similar data-gathering tools.

KEY CONTACTS

Madagascar Law Offices

Sahondra Rabenarivo
Managing Partner
T +(261) 20 23 25623
sahondra@madalaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MALAYSIA

Last modified 28 January 2019

LAW

Malaysia's first comprehensive personal data protection legislation, the Personal Data Protection Act 2010 (PDPA), was passed by the Malaysian Parliament on June 2, 2010 and came into force on November 15, 2013.

DEFINITIONS

Definition of personal data

'Personal data' means any information in respect of commercial transactions that is:

- Being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose
- Recorded with the intention that it should wholly or partly be processed by means of such equipment, or
- Recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, and, in each case

...that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user.

Personal data includes any sensitive personal data or expression of opinion about the data subject. Personal data does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

Definition of sensitive personal data

'Sensitive personal data' means any personal data consisting of information as to the physical or mental health or condition of a data subject, his or her political opinions, his or her religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him or her of any offense or any other personal data as the Minister of Communications and Multimedia (Minister) may determine by published order. Other than the categories of sensitive personal data listed above, the Minister has not published any other types of personal data to be sensitive personal data as of December 26, 2018.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to the PDPA, a Personal Data Protection Commissioner (Commissioner) has been appointed to implement the PDPA's provisions. The Commissioner will be advised by a Personal Data Protection Advisory Committee who will be appointed by the Minister, and will consist of one Chairman, three members from the public sector, and at least seven, but no more than eleven other members. The appointment of the Personal Data Protection Advisory Committee will not exceed a term of three years; however, members can be appointed for two successive terms.

The Commissioner's decisions can be appealed through the Personal Data Protection Appeal Tribunal. The following are examples of appealable decisions:

- Decisions relating to the registration of data users under Part II Division 2 of the PDPA
- The refusal of the Commissioner to register a code of practice under Section 23(5) of the PDPA
- The service of an enforcement notice under Section 108 of the PDPA
- The refusal of the Commissioner to vary or cancel an enforcement notice under Section 109 of the PDPA, or
- The refusal of the Commissioner to conduct or continue an investigation that is based on a complaint under Part VIII of the PDPA.

If a data user is not satisfied with a decision of the Personal Data Protection Advisory Committee, the data user may proceed to file a judicial review of the decision in the Malaysian High Courts.

REGISTRATION

Currently, the PDPA requires the following classes of data users to register under the PDPA:

1. **Communications**
    1. A licensee under the Communications and Multimedia Act 1998
    2. A licensee under the Postal Services Act 2012
2. **Banking and financial institution**
    1. A licensed bank and licensed investment bank under the Financial Services Act 2013
    2. A licensed Islamic bank and licensed international Islamic bank under the Islamic Financial Services Act 2013
    3. A development financial institution under the Development Financial Institution Act 2002
3. **Insurance**
    1. A licensed insurer under the Financial Services Act 2013
    2. A licensed takaful operator under the Islamic Financial Services Act 2013
    3. A licensed international takaful operator under the Islamic Financial Services Act 2013
4. **Health**
    1. A licensee under the Private Healthcare Facilities and Services Act 1998
    2. A holder of the certificate of registration of a private medical clinic or a private dental clinic under the Private Healthcare Facilities and Services Act 1998
    3. A body corporate registered under the Registration of Pharmacists Act 1951
5. **Tourism and hospitalities**
    1. A licensed person who carries on or operates a tourism training institution, licensed tour operator, licensed travel agent or licensed tourist guide under the Tourism Industry Act 1992
    2. A person who carries on or operates a registered tourist accommodation premises under the Tourism Industry Act 1992
6. **Transportation**
    1. Certain named transportations services providers
7. **Education**
    1. A private higher educational institution registered under the Private Higher Educational Institutions Act 1996
    2. A private school or private educational institution registered under the Education Act 1996
8. **Direct selling**
    1. A licensee under the Direct Sales and Anti-Pyramid Scheme Act 1993
9. **Services**
    1. A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961 carrying on business as follows:
        - legal
        - audit
        - accountancy
        - engineering
        - architecture

2. A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961, who conducts retail dealing and wholesale dealing as defined under the Control Supplies Act 1961
3. A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961, who carries on the business of a private employment agency under the Private Employment Agencies Act 1981

10. **Real estate**
    1. A licensed housing developer under the Housing Development (Control and Licensing) Act 1966
    2. A licensed housing developer under the Housing Development (Control and Licensing) Enactment 1978, Sabah
    3. A licensed housing developer under the Housing Developers (Control and Licensing) Ordinance 1993, Sarawak
11. **Utilities**
    1. Certain named utilities services providers
12. **Pawnbroker**
    1. A licensee under the Pawnbrokers Act 1972
13. **Moneylender**
    1. A licensee under the Moneylenders Act 1951

Certificates of registration are valid for at least one year, after which data users must renew registrations and may not continue to process personal data.

Data users are also required to display their certificate of registration at a conspicuous place at their principal place of business, and a copy of the certificate at each branch, where applicable.

The Commissioner may designate a body as a data user forum for a class of data users. Data user forums can prepare codes of practice to govern compliance with the PDPA, which can be registered with the Commissioner. Once registered, all data users must comply with the provisions of the code, and non-compliance violates the PDPA. As of December 26, 2018, the Commissioner has published several codes of practice, including for the banking and financial sector, the aviation sector, the utilities sector and the insurance and takaful industry in Malaysia.

DATA PROTECTION OFFICERS

Currently, Malaysian law does not require that data users appoint a data protection officer.

COLLECTION & PROCESSING

Under the PDPA, subject to certain exceptions, data users are generally required to obtain a data subject's consent for the processing (which includes collection and disclosure) of his or her personal data. Where consent is required from a data subject under the age of eighteen, the data user must obtain consent from the parent, guardian or person who has parental responsibility for the data subject. The consent obtained from a data subject must be in a form that such consent can be recorded and maintained properly by the data user.

Malaysian law contains additional data protection obligations, including, for example, a requirement to notify data subjects regarding the purpose for which their personal data are collected and a requirement to maintain a list of any personal data disclosures to third parties.

On December 23, 2015, the Commissioner published the Personal Data Protection Standard 2015 ("Standards"), which set out the Commission's minimum requirements for processing personal data. The Standards include the following:

- Security Standard For Personal Data Processed Electronically
- Security Standard For Personal Data Processed Non-Electronically
- Retention Standard For Personal Data Processed Electronically And Non-Electronically
- Data Integrity Standard For Personal Data Processed Electronically And Non-Electronically

TRANSFER

Under the PDPA, a data user may not transfer personal data to jurisdictions outside of Malaysia unless that jurisdiction has been specified by the Minister. However, there are exceptions to this restriction, including the following:

- The data subject has given his or her consent to the transfer.
- The transfer is necessary for the performance of a contract between the data subject and the data user.
- The data user has taken all reasonable steps and exercised all due diligence to ensure that the personal data will not be processed in a manner that would contravene the PDPA.
- The transfer is necessary to protect the data subject's vital interests.

In 2017, the Commissioner published a draft Personal Data Protection (Transfer of Personal Data to Places Outside Malaysia) Order 2017 to obtain public feedback on the proposed jurisdictions to which personal data from Malaysia may be transferred. As of December 26, 2018, the Minister has yet to approve the safe harbor jurisdictions. Once approved, a data user may transfer personal data to these safe harbor jurisdictions without having to rely on the data subject's consent or other prescribed exceptions under the PDPA.

SECURITY

Under the PDPA, data users have an obligation to take 'practical' steps to protect personal data, and in doing so, must develop and implement a security policy. The Commissioner may also, from time to time, set out security standards with which the data user must comply, and the data user is required to ensure that its data processors comply with these security standards.

In addition, the Standards provide separate security standards for personal data processed electronically and for personal data processed non-electronically (among others) and require data users to have regard to the Standards in taking practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

BREACH NOTIFICATION

There is no requirement under the PDPA for data users to notify authorities regarding data breaches in Malaysia. However, news reports dated October 5, 2018 suggest that Malaysia's laws could be updated, as early as the middle of 2019, to include data breach notification requirements modeled after those under the European Union's General Data Protection Regulation (GDPR), including requiring providing notice to government authorities.

ENFORCEMENT

Under the PDPA, the Commissioner is empowered to implement and enforce the personal data protection laws and to monitor and supervise compliance with the provisions of the PDPA. Under the Personal Data Protection Regulations 2013, the Commissioner has the power to inspect the systems used in personal data processing and the data user is required, at all reasonable times, to make the systems available for inspection by the Commissioner or any inspection officer. The Commissioner or the inspection officers may require the production of the following during inspection:

- The record of the consent from a data subject maintained in respect of the processing of that data subject's personal data by the data user
- The record of required written notices issued by the data user to the data subject
- The list of personal data disclosures to third parties
- The security policy developed and implemented by the data user
- The record of compliance with data retention requirements
- The record of compliance with data integrity requirements, and
- Such other related information which the Commissioner or any inspection officer deems necessary

Violations of the PDPA and certain provisions of the Personal Data Protection Regulations 2013 are punishable with criminal liability. The prescribed penalties include fines, imprisonment or both. Directors, CEOs, managers or other similar officers will have joint and several liability for non-compliance by the body corporate, subject to a due diligence defense.

However, there is no express right under the PDPA allowing aggrieved data subjects to pursue a civil claim against data users for

breaches of the PDPA.

ELECTRONIC MARKETING

The PDPA applies to electronic marketing activities that involve the processing of personal data for the purposes of commercial transactions. There are no specific provisions in the PDPA that deal with electronic marketing. However, the PDPA provides that a data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his or her personal data for direct marketing purposes. 'Direct marketing' means the communication by whatever means of any advertising or marketing material that is directed to particular individuals.

ONLINE PRIVACY

There are no provisions in the PDPA that specifically address the issue of online privacy (including cookies and location data). However, any electronic processing of personal data in Malaysia will be subject to the PDPA and the Commissioner may issue further guidance on this issue in the future.

KEY CONTACTS

Zaid Ibrahim & Co
www.zicolaw.com/

Sharon Tan
Partner
Zaid Ibrahim & Co
T +603 20879849
sharon.suyin.tan@zicolaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MALTA

Last modified 10 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The relevant law is the Data Protection Act 2018 (Act) (Chapter 586 of the Laws of Malta) and the Regulations (at present 11 in number) issued under it. The Act repealed and replaced the previous Data Protection Act (Chapter 440 of the Laws of Malta).

DEFINITIONS

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal**

convictions and offences (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Data Protection Act reproduces the definitions provided by Article 4, GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Information and Data Protection Commissioner (Commissioner). Informally, the Office of the Information and Data Protection Commissioner (OIDPC).

Level 2, Airways House
Second Floor
High Street
Sliema SLM 1549
Malta

T: +356 2328 7100
F: +356 23287198

idpc.info@idpc.org.mt

www.idpc.org.mt

The Commission has the function (among others) of generally protecting individuals' data protection rights against privacy violations in personal data processing.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Under Article 7 of the Maltese DPA, data controllers must consult and gain prior authorization from the Commissioner to process in the public interest: genetic data, biometric data or data concerning health for statisitical or research purposes or special categories of data relating to the management of social care services and systems.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Act does not derogate or further regulate from the provisions of the GDPR in this regard.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous,*" and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally

incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to re-purpose personal data – *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)

- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision taking, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (*ie,* opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The position under the Maltese Data Protection Act, 2018

The Act states that controllers and processors may derogate from the provisions of Articles 15, 16, 18 and 21 of the GDPR for the processing of personal data for scientific or historical research purposes or official statistics insofar as the exercise of the rights set out in those Articles:

1. Is likely to render impossible or seriously impair the achievement of those purposes, and
2. The data controller reasonably believes that such derogations are necessary for the fulfilment of those purposes.

Controllers and processors may also derogate from the obligations of Articles 15, 16, 18, 19, 20 and 21 of the GDPR for archiving purposes in the public interest. The same criteria ((1) and (2) above) must subsist for this derogation to apply.

Article 8 of the Act stipulates that an identity document shall only be processed when such processing is justified having regards to the purpose of processing and (1) the importance of a secure identification; or (2) any other valid reason as may be provided by law.

Personal data being processed for the purpose of exercising the right to freedom of expression and information, including processing for journalistic purposes or for the purpose of academic, artistic or literary expression, is exempt from compliance with the provisions of the GDPR (listed below), where, having regard to the right of freedom of expression and information in a democratic society, compliance with the following provisions would be incompatible with such processing purposes:

a. Chapter II (Principles)

- Article 5(1)(a) to (e) (principles relating to processing)
- Article 6 (lawfulness)
- Article 7 (conditions for consent)
- Article 10 (data relating to criminal convictions, etc.)
- Article 11(2) (processing not requiring identification)

b. Chapter III (rights of the data subject)

- Article 13(1) to (3) (personal data collected from data subject: information to be provided)
- Article 14(1) to (4) (personal data collected other than from the data subject)
- Article 15(1) to (3) (access to data and safeguards for third country transfers)

- Article 17(1) and (2) (right to erasure)
- Article 18(1)(a), (b) and (d) (restriction of processing)
- Article 20(1) and (2) (right to data portability)
- Article 21(1) (objections to processing)

c. Chapter IV (controller and processor)

- Article 25 (data protection by design and by default)
- Article 27 (representatives of controllers or processors not established in the Union)
- Article 30 (records of processing activities)
- Article 33 (notification of personal data breach to supervisory authority)
- Article 34 (communication of personal data breach to the data subject)
- Article 42 (certification)
- Article 43 (certification bodies)

d. Chapter VII (co-operation and consistency)

- Articles 60 to 62 (co-operation)
- Articles 63 to 67 (consistency)

Important note regarding age of consent: The processing of personal data of a child in relation to information society services has been lowered from eighteen (18) to thirteen (13) years of age by means of the 'Processing of Children's Personal Data in Relation to the Offer of Information Society Services Regulations' (Subsidiary Legislation 586.11 issued under the Data Protection Act 2018). It is important to note that the age of consent for valid contract formation in Malta remains 18 years of age. This grey area is still subject to local authoritative interpretation. We are not aware of any such interpretations at time of writing.

Finally, in certain circumstances, the collection and prcoessing of personal data are further regulated by local sector-specific regulations. By way of example, medical data relating to students can only be processed under specific conditions.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes, among others, binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
d. The transfer is necessary for important reasons of public interest

e. The transfer is necessary for the establishment, exercise or defense of legal claims
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
g. The transfer is made from a register, which according to EU or Member State law, is intended to provide information to the public, subject to certain conditions

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State (transfers in response to such requests where there is no other legal basis for transfer will infringe the GDPR).

The Act does not derogate or further regulate from the provisions of the GDPR in this regard.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

The Act does not derogate or further regulate from the provisions of the GDPR in this regard.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Act does not derogate or further regulate from the provisions of the GDPR in this regard.

The application form to be used when notifying data breaches to the OIDPC can be accessed here.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- Data subjects' rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The position under the Maltese Data Protection Act, 2018

Appealing against a decision of the Commissioner

Any person against whom an administrative fine has been imposed by the Commissioner may appeal to the Data Protection Appeals Tribunal within 20 days from service of the Commissioner's decision imposing such fine. An appeal to the Tribunal may be made on any of the following grounds:

- That a material error as to the facts has been made
- That there was a material procedural error
- That an error of law has been made
- That there was some material illegality, including unreasonableness or lack of proportionality

Within 2 days of filing an appeal, the Registry of the Tribunal shall:

- Serve a copy of the appeal on the Commissioner and request that he or she file a statement on the decision, together with any other information on which the decision was based within 20 days from the date on which the appeal was served
- Serve a copy of the appeal on the respondent(s) to the appealed decision, and request the respondent(s) file a reply within 20 days of service of the appeal

Appealing against a decision of the Data Protection Appeal Tribunal

Any party to an appeal before the Tribunal may appeal to the Court of Appeal by means of an application filed in the registry of that court within 20 days from the date on which the decision of the Tribunal was notified.

Fines against a public authority or body

The Commissioner may impose an administrative fine on a public authority or body of up to EUR 25,000 for each violation and an additional EUR 25 for each day during which such violation persists for an infringement under Article 83(4) of the GDPR. The fine that the Commissioner may impose on a public authority or body for an infringement of

Article 83(5) or (6) of the GDPR shall not exceed EUR 50,000 for each violation and additionally EUR 50 for each day during which such violation persists.

Any person who knowingly provides false information to the Commissioner when so requested or who does not comply with any lawful request pursuant to an investigation by the Commissioner, shall be guilty of an offence and upon conviction shall be liable to a fine (*multa*) of not less than EUR 1,250 and not more than EUR 50,000 or to imprisonment for six months.

Actions against a controller/processor

Without prejudice to any other available remedy, a person who believes that his or her rights under the GDPR or the Act have been infringed may file a sworn application in the First Hall Civil Court for an effective judicial remedy and in the same way may also institute an action for damages against the controller or processor who processes personal data in contravention of the provisions of the GDPR or this Act. If the court finds that the controller or processor is liable for damage caused pursuant to Article 82 of the GDPR, the court shall determine the amount of damages including, but not limited to, **moral damages**, due to the data subject.

Any action under Article 30 of this Act shall be instituted within 12 months from when the data subject became aware or should have reasonably become aware of such a contravention, whichever is earlier.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Act applies also to most electronic marketing activities since in the course of such activities, it is likely that 'personal data' as defined above (including email) will be 'processed' as understood by the Act. In relation to direct marketing (even electronic), consent may be revoked at will by the data subject(s).

The controller is legally bound to inform the data subject that he or she may oppose such processing at no cost.

Apart from the Act, the 'Processing of Personal Data (Electronic Communications Sector) Regulations' (Subsidiary Legislation 586.01 issued under the Data Protection Act 2018) (the Electronic Communications Regulations) address a number of activities relating specifically to electronic marketing.

In the case of subscriber directories, the producer of such directories shall ensure (without charge to the subscriber) that before any personal data relating to the subscriber (who must be a natural person) is inserted in the directory, the subscriber is informed about the purposes of such a directory of subscribers and its intended uses (including information regarding search functions embedded in the electronic version of the directories). No personal data shall be included

without the consent of the subscriber. In furnishing his consent the subscriber shall determine which data is to be included in the directory and is free to change, alter or withdraw such data at a later date. The personal data used in the directory must be limited to what is necessary to identify the subscriber and the number allocated to him, unless the subscriber has given additional consent authorizing the inclusion of additional personal data.

The Electronic Communications Regulations also deal with the issue of unsolicited communications. A person is prohibited from using any publicly available electronic communications service to engage in unsolicited communications for the purpose of direct marketing by means of:

- An automatic calling machine
- A facsimile machine
- Email

to a subscriber, irrespective of whether such subscriber is a natural person or a legal person, unless the subscriber has given his prior explicit consent in writing to the receipt of such a communication.

By way of exception to the above (informally known as the 'soft opt-in' rule), where a person has obtained from his customers their contact details for email in relation to the sale of a product or a service, in accordance with the Act that same person may use such details for direct marketing of its own similar products or services. However, the customers must be given the opportunity to object, free of charge and in an easy and simple manner, to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use.

In all cases the practice of, inter alia, sending email for the purposes of direct marketing, disguising or concealing the identity of the sender or without providing a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

The Act does not change the position under the previous Data Protection Act (Chapter 440) and does not introduce derogations from the provisions of the GDPR in this regard. The proposed ePrivacy Regulation would need to be analyzed separately.

ONLINE PRIVACY

Cookie Compliance

Subsidiary Legislation 586.01, entitled 'Processing of Personal Data (Electronic Communications Sector) Regulations' (recently renumbered to Subsidiary Legislation 586.01 from 440.01) amended the regulations implementing Article 2(5) of Directive 2009/136/EC into Maltese Law. However, the local Supervisory Authority (Commissioner) has not yet issued local guidelines on interpretation of the so called 'cookie clause'. It is unclear when, or if, such guidelines will be published. Of note, the Commissioner's website still makes reference to the Article 29 Data Protection Working Party Document 02/2013 providing guidance on obtaining consent for cookies (adopted on October 2, 2013).

Although the Act does not introduce new legislation in this regard, it is expected that GDPR consent rules will have an effect on cookie implementation in Malta.

Traffic Data

Under the Processing of Personal Data (Electronic Communications Sector) Regulations, traffic data relating to subscribers and users processed by an undertaking which provides publicly available electronic communications services or which provides a public communications network, must be erased or made anonymous when no longer required for the purpose of transmitting a communication.

Traffic data required for the purpose of subscriber billing or interconnection payments may be retained, provided however, that data retention is permissible only up to the period that a bill may lawfully be challenged or payment pursued.

Traffic data may be processed where the aim is to market or publicize the provision of a value-added service, however, the processing of such data shall only be permissible to the extent and for the duration necessary to render such services.

Processing of traffic data is also permissible by an undertaking providing publicly available electronic communication for the following purposes:

- Managing billing or traffic management
- Customer inquiries
- Fraud detection
- Rendering of value-added services

The Act does not introduce any new rules in this regard.

Location Data

Where location data (other than traffic data) relating to users or subscribers of public communications networks or of publicly available electronic communications services can be processed, such data may only be processed when it is made anonymous or with the consent of the users or subscribers, to the extent and for the duration necessary for the provision a value-added service.

Prior to obtaining user or subscriber consent, the undertaking providing the service shall inform them of the following:

- The type of location data which shall be processed
- The purpose and duration of processing
- Whether the processed data shall be transmitted to a third party for the purpose of providing the value-added service

A user or subscriber may withdraw consent for the processing of such location data (other than traffic data) at any time.

The Act does not change the previous position and does not derogate from the GDPR or further regulate in this regard.

KEY CONTACTS

Mamo TCV Advocates
www.mamotcv.com/

Dr. Antoine Camilleri
Partner
T +356 21 231 345
antoine.camilleri@mamotcv.com

Dr. Claude Micallef-Grimaud
Senior Associate
T +356 21 231 345
claude.micallefgrimaud@mamotcv.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MAURITIUS

Last modified 28 January 2019

LAW

Mauritius regulates data protection under the Data Protection Act 2017 (DPA 2017 or Act), proclaimed through Proclamation No. 3 of 2018, effective January 15, 2018. The Act repeals and replaces the Data Protection Act 2004, so as to align with the European Union General Data Protection Regulation 2016/679 (GDPR).

DEFINITIONS

Definition of personal data

Personal data is defined as any information relating to a data subject. Data subject means an natural person who is identified or identifiable, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Definition of sensitive personal data or special categories of personal data

Similar to the GDPR, the DPA 2017 refers to sensitive personal data as special categories of data. Special categories of data include personal data pertaining to any of the following about a data subject:

- Racial or ethnic origin
- Political opinion or adherence
- Religious or philosophical beliefs
- Membership of a trade union
- Physical or mental health or condition
- Sexual orientation, practices or preferences
- Genetic or biometric data that is uniquely identifying
- Commission or proceedings related to the commission of a criminal offense
- Such other personal data as the Commissioner may determine to be sensitive personal data

NATIONAL DATA PROTECTION AUTHORITY

Under DPA 2017, the Data Protection Office (DPO) is responsible for data protection oversight. The DPO is an independent and impartial public office that is not subject to the control or direction of any person or authority. The DPO is headed by the Data Protection Commissioner (Commissioner), with the assistance of public officers as may be necessary. The contact details of the DPO are:

Data Protection Office

5th Floor, SICOM Tower

Wall Street, Ebene

Republic of Mauritius

Tel: +230 460 0253

Fax: +230 489 7346

Web Address: http://dataprotection.govmu.org/

Email Address: dpo@govmu.org

REGISTRATION

Every person who intends to act as a data controller or a data processor (as defined below) must register with the Commissioner in a form approved by the Commissioner and may be required to pay a prescribed registration fee. The Commissioner is authorized to approve applications and issue registration certificates, which are valid for three years.

Data processors and controllers must renew their registration within three months prior to the date that their registration expires. Failure to register or renew registration constitutes an offense under the Act, punishable by a fine not to exceed ₨ 200,000 or imprisonment for a term not to exceed five years.

A data controller is a person or public body who alone, or jointly with others, determines the purposes and means of personal data processing, and who has decision making power with respect to processing. A data processor is a person or public body who processes personal data on behalf of a controller.

Application for registration

Every registration application must include all of the following:

- Name and address
- Whether a representative has been nominated for the purposes of the Act, and the name and address of the representative
- A description of the personal data to be processed by the controller or processor, and of the category of data subjects, to which the personal data relate
- A statement as to whether data controller or processor holds, or is likely to hold, special categories of personal data
- A description of the purpose for which the personal data are to be processed
- A description of any recipient to whom the controller intends or may wish to disclose the personal data
- The name, or a description of, any country to which the proposed controller intends or may wish, directly or indirectly, to transfer, the data
- A general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the personal data

A controller or processor who knowingly supplies false or misleading material information in their registration application commits an offense and could be held liable to a fine not to exceed ₨ 100,000 or imprisonment for a term not to exceed five years.

DATA PROTECTION OFFICERS

Yes, controllers must appoint data protection officers.

The DPA 2017 provides that every controller shall adopt policies and implement appropriate technical and organizational measures so as to ensure and be able to demonstrate that the processing of personal data is performed in accordance with this Act.

Measures must include the designation of a data protection officer who is responsible for compliance issues related to data collection and processing.

COLLECTION & PROCESSING

Unless an exemption applies, a controller cannot collect personal data unless the collection (a) is for a lawful purpose connected with a function or activity of the data controller, and (b) the collection is necessary for that purpose.

Where the data controller collects personal data directly from the data subject, the data controller shall at the time of collecting personal data ensure that the data subject concerned is informed of:

- The identity and contact details of the controller and, where applicable, its representative and any data protection officer
- The purpose for which the data are being collected
- The intended recipients of the data
- Whether or not the supply of the data by that data subject is voluntary or mandatory
- The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The existence of the right to request from the controller access to and rectification, restriction or erasure of personal data concerning the data subject or to object to the processing
- The existence of automated decision making, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
- The period for which the personal data shall be stored
- The right to lodge a complaint with the Commissioner
- Where applicable, that the controller intends to transfer personal data to another country and on the level of suitable protection afforded by that country
- Any further information necessary to guarantee fair processing in respect of the data subject's personal data, having regard to the specific circumstances in which the data are collected

Where data is not collected directly from the data subject concerned, the data controller or any person acting on his behalf shall ensure that the data subject is informed of the matters set out above.

Every controller or processor shall ensure that personal data are:

- Processed lawfully, fairly and in a transparent manner in relation to any data subject
- Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the

personal data are processed, and

- Processed in accordance with the rights of data subjects

According to the DPA 2017, no person shall process personal data unless the data subject consents to the processing for one or more specified purposes or a specific exception (as listed below). Consent must be freely given, specific, informed and an unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which he signifies his agreement to personal data relating to him being processed.

The exceptions to the requirement of consent are when the processing is necessary for any of the following:

- The performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract
- Compliance with any legal obligation to which the controller is subject
- In order to protect the vital interests of the data subject or another person
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- The performance of any task carried out by a public authority
- The exercise, by any person in the public interest, of any other functions of a public nature
- The legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject
- The purpose of historical, statistical or scientific research

Special categories of personal data

As a general rule, special categories of personal data cannot be processed unless the individual has given his affirmative consent to the processing or one or more of the exceptions apply in addition to any of the following applying:

- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for: (i) the establishment, exercise or defense of a legal claim; (ii) the purpose of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to a contract with a health professional subject to the obligation of professional secrecy; (iii) the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; or (iv) protecting the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent

TRANSFER

A controller or processor may transfer personal data to another country where any of the following apply:

- It has provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data
- The data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards

- The transfer is necessary: (i) for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person; (iii) for reasons of public interest as provided by law; (iv) for the establishment, exercise or defense of a legal claim; or (v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or (vi) for the purpose of compelling legitimate interests pursued by the controller or the processor which are not overridden by the interests, rights and freedoms of the data subjects involved and where – (A) the transfer is not repetitive and concerns a limited number of data subjects; and (B) the controller or processor has assessed all the circumstances surrounding the data transfer operation and has, based on such assessment, provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data
- The transfer is made from a register which, according to law, is intended to provide information to the public and which is open for consultation by the public or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down by law for consultation are fulfilled in the particular case. Such transfer a shall not involve the entirety of the personal data or entire categories of the personal data contained in the register and, where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or in case they are to be the recipients

The Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the safeguards or the existence of compelling legitimate interests and may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as he may determine.

SECURITY

Under the DPA 2017, a controller or processor must implement and maintain appropriate security and organizational measures for the prevention of unauthorized access to, alteration, disclosure or destruction of, or the accidental loss of the personal data.

Additionally, the controller or processor must ensure that measures provide a level of security appropriate to the harm that may result from the unauthorized access to, alteration, disclosure or destruction of, or the accidental loss of the personal data and the nature of the personal data concerned.

The measures referred to above shall include all of the following:

- The pseudonymization and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

In determining the appropriate security measures, in particular, where the processing involves the transmission of data over an information and communication network, a data controller shall have regard to the:

- State of technological development available
- Cost of implementing any of the security measures
- Special risks that exist in the processing of the data, and
- Nature of the data being processed

Where a controller is using the services of a processor – (a) the controller must choose a processor that is able to provide sufficient guarantees in respect of security and organizational measures for the purpose of complying with the security measures described above; and (b) the controller and the processor shall enter into a written contract which shall provide that – (i) the processor shall act only on instructions received from the controller; and (ii) the processor shall be bound by obligations of the controller as regards security measures to be taken.

If the purpose for keeping personal data has lapsed, the controller must destroy such data as soon as reasonably practicable and notify any data processor holding such data, who in turn must destroy the data specified by the controller as soon as is reasonably

practicable.

Every controller or processor has to take all reasonable steps to ensure that any person employed by him or it is aware of, and complies with, the relevant security measures.

BREACH NOTIFICATION

Under the DPA 2017, a personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

A controller must without undue delay and, where feasible, not later than 72 hours after having become aware, provide the Commissioner with notice of a personal data breach. Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the controller shall also communicate the personal data breach to the data subject without undue delay.

ENFORCEMENT

The DPA 2017 provides the Commissioner with enforcement authority. The Commissioner may investigate complaints that the Act or its subordinate regulations has been or is being violated, the Commissioner authorizes an officer to investigate the complaint or cause, unless he is of the opinion that the complaint is frivolous or vexatious.

If the Commissioner is unable to arrange an amicable resolution for the parties concerned within a reasonable time frame, the Commissioner shall notify, in writing, the individual who made the complaint of the Commissioner's decision. Commissioner decisions may be appealed under Section 51 of the Act.

If the Commissioner is of the opinion that a controller or a processor has contravened, is contravening or is about to contravene the DPA 2017, the Commissioner may serve an enforcement notice on the data controller or processor, requiring remedial efforts within a specified time frame.

A person who, without reasonable excuse, fails or refuses to comply with an enforcement notice commits an offense, and, on conviction, is liable to a fine not to exceed ₨50,000 and to imprisonment for a term not to exceed two years.

If the Commissioner has reasonable grounds to believe that data is vulnerable to loss or modification, she may make an application to a Judge in Chambers for an order for the expeditious preservation of such data.

The Commissioner may also carry out periodical audits of the systems and security measures of data controllers or data processors to ensure compliance with data protection principles laid down in the DPA 2017.

ELECTRONIC MARKETING

The Act regulates direct marketing, which is defined as the communication of any advertising or marketing material which is directed to a particular individual. The definition also encompasses electronic marketing.

The data subject may object to the processing of his or her personal data for purposes of direct marketing, including profiling to the extent relevant. Where a data subject objects to processing, his or her personal data may no longer be processed for that purpose.

ONLINE PRIVACY

The Act applies to online privacy, though it does not contain specific provisions in relation to online privacy.

KEY CONTACTS

Juristconsult Chambers

Shalinee Dreepaul Halkhoree
Partner-Barrister
T +230 465 00 20 Extension 225
sdreepaul@juristconsult.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MEXICO

Last modified 28 January 2019

LAW

The Federal Law on the Protection of Personal Data held by Private Parties (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*) ("the Law") entered into force on July 6, 2010.

The Executive Branch has also issued:

- The Regulations to the Federal Law on the Protection of Personal Data held by Private Parties (*Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*) (the Regulations), which entered into force on December 22, 2011
- The Privacy Notice Guidelines (the Guidelines), which entered into force on April 18, 2013
- The Recommendations on Personal Data Security, on November 30, 2013
- The Parameters for Self-Regulation regarding personal data, which entered into force on May 30, 2014
- The General Law for the Protection of Personal Data in Possession of Obligated Subjects *(Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*), which entered into force on January 27, 2017

On June 12, 2018, a decree was published in the Official Gazette of the Federation approving two important documents: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data dated January 28, 1981, and its Additional Protocol regarding supervisory authorities and trans-border data flows dated November 8, 2001.

The Regulations apply to all personal data processing when:

- Processed in a facility of the data controller located in Mexican territory
- Processed by a data processor, regardless of its location, if the processing is performed on behalf of a Mexican data controller
- Where the Mexican legislation is applicable as a consequence of Mexico's adherence to an international convention or the execution of a contract (even where the data controller is not located in Mexico), or
- Where the data controller is not located in Mexican territory, but uses means located in Mexico to process personal data, unless such means are used only for transit purposes

The Law only applies to private individuals or legal entities that process personal data, and not to the government, credit reporting companies governed by the Law Regulating Credit Reporting Companies or persons carrying out the collection and storage of personal data exclusively for personal use where it is not disclosed for commercial use.

DEFINITIONS

Definition of personal data

'Personal Data' is any information concerning an identified or identifiable individual.

Definition of sensitive personal data

'Sensitive Personal Data' is personal data that affects the most intimate areas of the data subject's life, which if misused, may lead to discrimination or entail a serious risk to the data subject. In particular, the definition includes data that may reveal any of the following:

- Racial or ethnic origin
- Past or present health conditions
- Genetic information
- Religious, philosophical or moral beliefs
- Union affiliation
- Political views
- Sexual orientation
- Pictures and videos
- Fingerprints
- Geolocation
- Banking information
- Signature

NATIONAL DATA PROTECTION AUTHORITY

The National Institute of Transparency for Access to Information and Personal Data Protection (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*) (INAI) and the Ministry of Economy (*Secretaría de Economía*) serve as Mexico's data protection authorities.

REGISTRATION

Mexican law does not require registration with a data protection authority or other regulator in relation to the use of personal data.

DATA PROTECTION OFFICERS

All data controllers are required to designate a personal data officer or department (each, a Data Protection Officer) to handle requests from data subjects exercising their ARCO Rights (as defined in 'Collection and Processing') under the Law. Data Protection Officers are also responsible for enhancing the protection of personal data within their organizations.

COLLECTION & PROCESSING

The term 'processing' is broadly defined to include the collection, use, communication or storage of personal data by any means. Use includes all access, management, procurement, transfer and disposal of personal data.

In processing personal data, data controllers must observe the principles of legality, information, consent, notice, quality, purpose, loyalty, proportionality and accountability.

Personal data must be:

- Collected and processed fairly and lawfully
- Collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes
- Adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed
- Accurate and, if necessary, updated; every reasonable step must be taken to ensure that data that is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified, and
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed

Data subjects are entitled to a reasonable expectation of privacy in the processing of their personal data. In addition, personal data must be processed as agreed upon by the parties (in a privacy notice or otherwise) and in compliance with the Law.

To legally process personal data, data controllers must provide a privacy notice (Aviso de Privacidad) (the Privacy Notice), which must be made available to a data subject prior to the processing of his or her personal data. The Privacy Notice may be provided to data subjects in printed, digital, visual or audio formats, or any other technology.

A comprehensive Privacy Notice must at least contain:

- The identity and domicile of the data controller collecting the data
- The purposes of the data processing
- The options and means offered by the data controller to data subjects to limit the use or disclosure of their data
- The means for exercising rights of access, rectification, cancellation or objection (ARCO rights) in accordance with the provisions of the Law
- Where appropriate, the types of data transfers to be made
- The procedure and means by which the data controller will notify the data subjects of changes to the Privacy Notice, and
- Identification of any sensitive personal data that will be processed

The Guidelines permit the following three forms of privacy notice: comprehensive, simplified and short form, depending on whether the personal data is obtained directly or indirectly from the data subject, and the context and space in which the personal data is collected. Each of these forms must meet specific disclosure requirements.

The data controller has the burden of proof to show that the Privacy Notice was provided to the data subject prior to the processing of his or her personal data.

Some form of consent is required for all processing of personal data, except as otherwise provided by the Law. Implicit consent (notice and opt-out) applies to the processing of personal data generally; express consent (notice and opt-in) applies to the processing of financial or asset data; and express and written consent applies to the processing of sensitive personal data. Consent may be communicated verbally, in writing, or via any technology, or by any other unmistakable indication. Express written consent may be obtained through the data subject's written signature, electronic signature, or any other authentication mechanism.

Consent from the data subject will not be required for the processing of personal data in any of the following apply:

- Any law so provides
- The data is contained in publicly available sources
- The identity of the data subject has been disassociated from the data
- Processing has the purpose of fulfilling obligations under a legal relationship between the data subject and the data controller
- There is an emergency situation that could potentially harm an individual with regard to his or her person or property
- Processing is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the data subject is unable to give consent in the manner established by the General Health

Law (*Ley General de Salud*) and other applicable laws, and said processing is carried out by a person subject to a duty of professional secrecy or an equivalent obligation, or

- Pursuant to a resolution issued by a competent authority

TRANSFER

Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide the third parties with the Privacy Notice provided to the data subject and the purposes to which the data subject has limited the data processing.

Data processing must be consistent with what was agreed in the Privacy Notice, which shall contain a clause indicating whether or not the data subject agrees to the transfer of his or her data. The third party recipient assumes the same obligations as the data controller who has transferred the data.

Domestic or international transfers of personal data may be carried out without the consent of the data subject where the transfer is:

- Pursuant to a law or treaty to which Mexico is party
- Necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management
- Made to the holding company, subsidiaries or affiliates under the common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies as the data controller
- Necessary by virtue of a contract executed or to be executed between the data controller and a third party in the interest of the data subject
- Necessary or legally required to safeguard public interest or for the administration of justice
- Necessary for the recognition, exercise or defense of a right in a judicial proceeding, or
- Necessary to maintain or comply with an obligation resulting from a legal relationship between the data controller and the data subject.

The Regulations establish that communications or transmissions of personal data to data processors do not need to be informed nor consented by the data subject. However, the data processor must do all of the following:

- Process personal data only according to the instructions of the data controller
- Not process personal data for a purpose other than as instructed by the data controller
- Implement the security measures required by the Law, the Regulations and other applicable laws and regulations
- Maintain the confidentiality of the personal data subject to processing
- Delete personal data that were processed after the legal relationship with the data controller ends or when instructed by the data controller, unless there is a legal requirement for the preservation of the personal data
- Not transfer personal data unless instructed by the data controller, the communication arises from subcontracting, or if so required by a competent authority

SECURITY

All data controllers must establish and maintain physical, technical and administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorized use, access or processing. They may not adopt security

measures that are inferior to those they have in place to manage their own information.

The risk involved, potential consequences for the data subjects, sensitivity of the data and technological development must be taken into account when establishing security measures.

BREACH NOTIFICATION

Security breaches occurring at any stage of the processing that materially affect the property or moral rights of the data subject must be promptly reported by the data controller to the data subject.

The Regulations provide that breach notification must include at least the following information:

- The nature of the breach
- The personal data compromised
- Recommendations to the data subject concerning measures that he or she can adopt to protect his or her interests
- Corrective actions implemented immediately, and
- The means by which the data subject may obtain more information in regard to the data breach

ENFORCEMENT

Data subjects can enforce their ARCO Rights, when no response is obtained from the data controller via INAI and ultimately the court system.

If any breach of the Law or its Regulations is alleged, INAI may perform an on-site inspection at the data controller's facilities to verify compliance with the Law.

Violations of the Law may result in monetary penalties or imprisonment, including the following:

- INAI may impose monetary sanctions in the range of 100 to 320,000 times the Mexico City minimum wage (currently, MX$88.36, updated every year). Sanctions may be increased up to double the above amounts for violations involving sensitive personal data.
- Three months to three years of imprisonment may be imposed on any person authorized to process personal data who, for profit, causes a security breach affecting the databases under its custody. Penalties will be doubled if sensitive personal data is involved.
- Six months to five years of imprisonment may be imposed on any person who, with the aim of obtaining unlawful profit, processes personal data deceitfully, taking advantage of an error of the data subject or a person authorized to process such data. Penalties will be doubled if sensitive personal data is involved.

ELECTRONIC MARKETING

Email marketing constitutes personal data processing and is subject to the Law, including applicable notice and consent requirements.

ONLINE PRIVACY

The Regulations and Guidelines that address the use of cookies, web beacons and other analogous technologies, require that when a data controller uses online tracking mechanisms that permit the automatic collection of personal data, it provides prominent notice of the use of such technologies; the fact that personal data is being collected the type of personal data collected and the purpose of the collection and the options to disable such technologies.

An IP address alone may be considered personal data, however, there has not been a resolution or decision issued by the

competent authority on this point.

KEY CONTACTS

Gabriela Alaña
Partner
T + 52 55 5261.1817
gabriela.alana@dlapiper.com

Ana Kuri
Associate
T + 52 55 5261.1847
ana.kuri@dlapiper.com

Paola Aguilar
Law Clerk
T +1 555.261.1818
maria.aguilar@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MONACO

Last modified 28 January 2019

LAW

Within the Principality of Monaco (Monaco) data protection is regulated by Data Protection Law n° 1.165 of December 23, 1993, modified from time to time and notably by Law n° 1.353 of December 4, 2008 and most recently by Law n°1.462 of June 28, 2018 (DPL).

Further, Monaco is part of the Council of Europe and entered into Convention n° 108 of the European Council. However, Monaco is not part of the EU and did not adopt Data Protection Directive 95/46/EC or its successor the General Data Protection Regulation.

DEFINITIONS

Definition of personal data

Under the DPL, personal data is defined as data enabling identification of a determined or indeterminable person. Any individual who can be identified, directly or indirectly, notably by reference to an identification number or to one or more factors specific to their physical, psychological, psychological, economic, cultural, or social identity is deemed to be identifiable.

Definition of sensitive personal data

While not expressly defined under the DPL, sensitive personal data is considered to be personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health / genetic data, sex life, data concerning morals or social matters.

NATIONAL DATA PROTECTION AUTHORITY

The Monegasque regulator is the Commission for Control of Personal Data (*Commission de Contrôle des Informations Nominatives* or "CCIN").

REGISTRATION

Data controllers, who process personal data must notify the CCIN and request approval so that their processing of personal data may be registered. Any changes to the processing of personal data will require the registration to be amended.

The notification to the CCIN should include the following information:

- What data is being collected
- Why the data will be processed

- The categories of data subject
- Whether the data will be transferred either within or outside the Monaco

DATA PROTECTION OFFICERS

There is no requirement in Monaco for organizations to appoint a data protection officer.

However, appointing a data protection officer is viewed by the CCIN as evidence of a company's measure taken in order to ensure compliance with the data protection legislation. In practice however, companies in Monaco do not generally appoint data protection officers.

COLLECTION & PROCESSING

Data processing must be justified by at least one of the following bases:

- The data subject's consent
- A legal duty imposed to the data controller
- A public purpose
- The performance of a contract entered into between the data controller and the data subject
- The data controller's legitimate interests, unless the data subject's fundamental rights and liberties outweigh the controller's legitimate interests

If sensitive personal data is processed, at least one of the above bases must be met plus one from an additional list of more stringent conditions.

Additionally, the data controller must provide the data subject with fair processing information. This includes information about the identity of the data controller, the purposes of processing and any other information needed under the circumstances to ensure that the processing is fair.

TRANSFER

Monaco is not part of the EU, so the DPL does not distinguish between EEA jurisdictions and non-EEA jurisdictions.

However, the DPL provides that the transfer of data is authorized for cross-border access, storage and processing of data only to a country which offers equivalent data protection and reciprocity.

The CCIN has established a list of the countries deemed to offer equivalent protection and reciprocity. States, and parties to the Convention of the Council of Europe n° 108 relating to the protection of individuals for personal data automatic processing, are deemed to have the equivalent protection as Monaco.

Data transfers to countries with an adequate level of protection are not subject to the authorization by the CCIN.

The CCIN has adopted a position of principle and decided that all personal data transfers to a country or an organization which does not ensure an adequate level of protection should, in any event, be submitted to the Commission in the form of a transfer authorization application. Subsequently, the CCIN affirmed that it is necessary to submit a transfer authorization application to the Commission if personal data will be accessed from a country that does not have an adequate level of protection.

SECURITY

Data controllers must take appropriate technical and organizational measures designed to protect against unauthorized or unlawful processing, accidental loss or destruction of, or damage to, personal data. The measures taken must ensure a level of

security appropriate to the harm which might result from such unauthorized or unlawful processing or accidental loss, destruction or damage as mentioned above, and must be appropriate to the nature of the personal data.

Measures implemented must ensure an adequate level of security with regard to the risks posed by processing and by the nature of the data to be protected.

Where the data controller or their representative engages a service provider to process personal data, they must ensure that the service provider is able to comply with the obligations laid down in the two previous paragraphs.

BREACH NOTIFICATION

There is no mandatory requirement in the DPL to report security breaches or losses to the CCIN or to data subjects.

ENFORCEMENT

The CCIN and Monegasque Courts are responsible for enforcing the DPL. If the CCIN becomes aware that a data controller is in breach of the DPL, it can serve an enforcement notice requiring the data controller to resolve the non-compliance. Failure to comply with an enforcement notice is a criminal offense and can be punished on conviction with imprisonment of one month to one year or a fine of between €9,000 and €90,000 or both.

ELECTRONIC MARKETING

Prior to implementing any electronic marketing activity the CCIN must be notified, as electronic marketing activities may use personal data. The DPL does not prohibit the use of personal data for the purpose of electronic marketing *per se*. However, when implementing electronic marketing activities a company must respect the provisions of Articles 1, 10-1, 10-2 and 14 of the DPL.

The automated or non-automated processing of personal data must not infringe the fundamental rights and freedoms enshrined in Title III of the Constitution.

When marketing, personal data must be:

- Collected and processed fairly and lawfully
- Collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes
- Adequate, relevant and not excessive in relation to the purposes for which it is collected and / or further processed
- Accurate and, if necessary, updated; every reasonable step must be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.

Processing of personal data must be justified by one of the following bases:

- By consent from the data subject(s)
- By compliance with a legal obligation to which the data controller or their representative is subject
- By it being in the public interest
- By the performance of a contract or pre-contractual measures with the data subject

- By the fulfillment of a legitimate motive on the part of the data controller or their representative or by the recipient, on condition that the interests or fundamental rights and freedoms of the data subject are not infringed

Data subjects from whom personal data is collected must be informed of all of the following:

- The data controller's identity and, if applicable, the identity of their representative in Monaco
- The purpose of processing
- The obligatory or optional nature of replies
- The consequences for data subjects of failure to reply
- The identity of recipients or categories of recipients
- Their right to oppose, access and rectify their data
- Their right to oppose disclosure to and use of personal data by a third party, or the disclosure for the purposes of the third party's commercial use, including marketing

ONLINE PRIVACY

Prior to the use of traffic data, location data and cookies the CCIN must be notified. The use of traffic data, location data and cookies will have to comply with the provisions of the DPL.

KEY CONTACTS

Gordon S. Blair Law Offices
gordonblair.com/

Gilbert Delacour
CEO
Gordon S. Blair Law Offices
T +377 93 25 84 00
gilbertdelacour@gordonblair.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MONTENEGRO

Last modified 28 January 2019

LAW

The Law on Protection of Personal Data, Official Journal of Montenegro, nos. 79/2008, 70/2009, 44/2012 and 22/2017, (DP Law) is the governing data protection law. It was first enacted in December 2008 and last amended in March of 2017.

The Montenegrin Parliament is expected to adopt a new Data Protection Law within the next six months, to harmonize its data protection law with the EU General Data Protection Regulation (GDPR). However, currently no draft or proposal of this new law exists.

DEFINITIONS

Definition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable data subject. Data subjects are natural persons whose identity is or can be determined, directly or indirectly, in particular by reference to a personal identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

Under the DP Law, sensitive personal data is data relating to:

- Ethnicity or race
- Political opinion, or religious or philosophical belief
- Trade union membership
- Information on health condition and sexual life

NATIONAL DATA PROTECTION AUTHORITY

The Agency for Protection of Personal Data and Free Access to Information (DPA) is the local data protection authority. The DPA is currently located at:

Bulevar Svetog Petra Cetinjskog 147 Podgorica

For more information see the DPA's website at www.azlp.me

REGISTRATION

Each data controller must do the following:

- Register as a data controller (this registration as a controller is to be performed only once)
- Separately register each database of personal data ('Database') which it intends to establish, before the database is established.

Both registrations must be submitted online through specific forms, which are accessible via the DPA's website. The type and scope of the information that must be included in these forms is explicitly prescribed by the DP Law (*eg*, the data controller's name and address of its registered seat, name of the Database, legal basis for the processing and purpose of the processing, types of processed data, categories of data subjects, (if applicable) information on any data transfers out of Montenegro). Any significant change to the registered data processing activities, subsequent to the registration should be notified to and registered with the DPA as well.

Exceptionally (*ie*, if the intended data processing represents a special risk for the rights and freedoms of individuals), a data controller may, depending on the circumstances of each particular case, be obliged to obtain the DPA's prior approval for such processing (*eg*, if biometric data is to be processed without the data subject's consent).

DATA PROTECTION OFFICERS

Under the DP Law, a data controller is required to appoint a DPO subsequent to the Database's establishment. However, a DPO is not required if the data controller has less than ten employees involved in the processing of personal data.

COLLECTION & PROCESSING

A prerequisite for the legitimate processing of personal data is to obtain the data subject's valid, informed consent. The consent requirements are explicitly described in the DP Law (*eg*, data subjects have to be informed about the purpose and legal basis for the respective processing). The processing of personal data without consent is only allowed under the exceptions listed in the DP Law, *(eg,* if the processing is necessary to meet the data controller's statutory obligations under the law or for the protection of life and other vital interests of the data subject who is not capable to personally consent).

As a general matter, in order to comply with the provisions under the DP Law, the processing has to be done in a fair and lawful manner, the type and scope of processed data must be proportionate to the purpose of the respective processing, the data should not be retained longer than necessary in order to meet the defined purpose, and the data has to be accurate, complete and up-to-date.

TRANSFER

Under the DP Law, personal data may be transferred to countries or international organizations, where an adequate level of personal data protection exists, subject to the DPA's approval. The DPA issues such approval only where it establishes that adequate measures for the protection of personal data are undertaken (criteria for the adequacy assessment include, for example, the type of the data and the statutory rules in force in the country to which the data is to be transferred).

However, in certain cases the DPA's approval is not required for data transfers out of Montenegro, as explicitly prescribed by the DP Law *(eg,* if the data subject consented to the transfer and was made aware of possible consequences of such transfer, or the data is transferred to the European Union or European Economic Area or to any country that the EU Commission has determined ensure adequate level of the data protection).

SECURITY

The DP Law requires that both data controllers and processors undertake technical, personnel and organizational measures for the protection of personal data against loss, destruction, unauthorized access, alteration, publication and misuse. Further, individuals who process personal data are required to keep the processed personal data confidential.

Additionally, data controllers are required to establish internal rules regarding their personal data processing and protection of same (which should include identifying the measures undertaken). Data controllers should also determine which employees have

access to the processed data (and to which of this data), as well as the types of data which may be disclosed to other users (and the conditions for the respective disclosure). Finally, if the processing is performed electronically, a data controller is required to ensure that certain information on the use and recipients of the respective data, is automatically kept in the information system.

BREACH NOTIFICATION

There is no data security breach notification requirement under the DP Law. However, the Law on Electronic Communications ('Official Journal of Montenegro', nos. 40/2013, 56/2013 and 2/2017) ('EC Law') does impose a duty on operators to, without undue delay, notify the Montenegrin Agency for Electronic Communications and Postal Activity (EC Agency) and the DPA of any breach of personal data or privacy of the data subjects. The affected data subject should also be notified if the breach may have a detrimental effect to their personal data or privacy (unless the EC Agency issues an opinion that such notification is not needed). Failure to comply with any of the above duties is subject to liability and fines, ranging from €6,000 to €30,000 for a legal entity, and from €300 to €3,000 for a responsible person within a legal entity, and, if some material gain was obtained through the violation, the protective measure, which includes seizure of the respective gain, may be imposed in addition to the above monetary fine.

ENFORCEMENT

The DPA is the competent authority for the DP Law's enforcement. It is authorized and obliged to monitor implementation of the DP Law, both ex officio, and upon a third party complaint.

When monitoring the DP Law's implementation, the DPA is authorized to pass the following decisions:

- Order removal of the existing irregularities within certain period of time
- Temporarily ban the processing of personal data which is carried out in violation of the DP Law
- Order deletion of unlawfully collected data
- Ban transfer of data outside of Montenegro or its disclosure to data recipients carried out in violation of the DP Law
- Ban data processing by an outsourced data processor if it does not fulfill the data protection requirements or if its engagement as a data processor is carried out in violation of the DP Law
- Ban data processing by an outsourced data processor if it does not fulfil the data protection requirements or if its engagement as a data processor is carried out in contravention to the DP Law.

The DPA's decisions may not be appealed, but an administrative dispute before the competent court may be initiated against the same.

The DPA may also file a request for the initiation of civil proceeding. The offenses and sanctions are explicitly prescribed by the DP Law, which includes monetary fines ranging from €500 to €20,000 for a legal entity and ranging from €150 to €2,000 for a responsible person in a legal entity.

There exists potential criminal liability. The unauthorized collection and use of personal data is a criminal offense under the Montenegrin Criminal Code, punishable with a monetary fine (in an amount to be determined by the court) or imprisonment up to one year. Both natural persons and legal entities can be subject to criminal liability.

ELECTRONIC MARKETING

Electronic marketing is not governed by the DP Law. Nevertheless, this law does govern protection of personal data used in direct marketing. In that regard, the law requires that data subjects have to be provided with a possibility to object to the processing of their personal data for direct marketing purposes prior to the commencement of the respective processing. Regarding the use of sensitive personal data in direct marketing, it is explicitly prescribed that a data subject's consent is a requirement for the respective processing.

Although not governed by the DP Law, there are other regulations which govern electronic marketing, including the Law on Electronic Trade ('Official Journal of the Republic of Montenegro', no. 80/04 and 'Official Journal of Montenegro', nos. 41/10, (…), 56/13) ('ET Law'). In this respect, one of the most important rules prescribed by the ET Law is the rule that any sending of unsolicited commercial messages is not allowed unless prior consent of the recipients of the respective marketing is obtained. It is

strictly forbidden to send any marketing messages to individuals who have indicated that they do not want to receive such *(ie,* opted-out) (and a service provider who sends unsolicited commercial messages is required to establish and maintain a record of individuals who opted-out). A violation of the respective rules is subject to liability, with fines ranging from €500 to €17,000 (for a legal entity) and ranging from €100 to €1,500 (for a responsible person in a legal entity). For particularly serious violations or repeated violations, an order banning or suspending the business activity (lasting from three months to six months) may be imposed on an entity responsible for the respective violations).

ONLINE PRIVACY

There is no specific law or regulation explicitly governing online privacy, including cookies. Accordingly, the general data protection rules, as introduced by the DP Law are applicable to online privacy, to the extent personal data is processed.

On the other hand, the EC Law, as defined in the ***Breach Notification*** section above, introduces relevant rules that are mandatory for the operators under this law. For example, a public electronic communication services' user is particularly entitled to the protection of their electronic communications' secrecy in compliance with the DP Law.

Further, the EC Law imposes explicit rules on traffic data and location data. Under these rules, operators are:

- Required to retain certain traffic data and location data for certain purposes explicitly set out by the law (for example, for the detection and criminal prosecution of criminal offenders), whereas the retention period should last at least six months and would not be longer than two years ('Retention Obligation'), keeping in mind that this obligation does not apply to data which reveals a content of electronic communications.
- Regarding traffic data related to subscribers/users which is not subject to the Retention Obligation, an operator is required to delete this data if it is no longer needed for the communication's transmission or can keep it, but only if it modifies the respective data in a way that it cannot be linked to a particular person. Apart from this, it is also prescribed that:
    - If the traffic data's retention purpose is to use it for the calculation of the costs of the relevant services/interconnection, it can be retained for as long as claims regarding the respective costs can legally be requested, but under condition that an user is informed on its processing's purpose and duration, and that
    - If the traffic data's processing purpose is to promote and sell electronic communication services or to provide value added services, such processing is allowed, but only with the data subjects' prior consent (which can be withdrawn at any time)
- Regarding location data which is not subject to the Retention Obligation, an operator is allowed to process it but only with the data subject's consent (which can be withdrawn at any time) or if the respective data is modified in a way that it cannot be linked to a particular person without consent.

Failure to comply with any of the above rules regarding the processing of traffic or location data which is not covered by the above-identified Retention Obligation, is subject to offence liability and fines in range from €4,000 to €20,000 for a legal entity, and in range from €200 to €2,000 for a responsible person in a legal entity.

KEY CONTACTS

Karanovic & Nikolic
www.karanovic-nikolic.com/

Milena Ronevi
Associate
T office +382 20 238 991
milena.roncevic@karanovic-nikolic.com

Sanja Spasenovic
Attorney at law in cooperation with Karanovic & Partners
Karanovic & Partners
T Office +381 11 3094 200/ Direct T +381 11 3955 413
Sanja.Spasenovic@karanovicpartners.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MOROCCO

Last modified 28 January 2019

LAW

Morocco's law governing privacy and data protection is Law No 09-08, dated February 18, 2009 relating to protection of individuals with regard to the processing of personal data and its implementation Decree n° 2-09-165 of May 21, 2009 (together the DP Law).

DEFINITIONS

Definition of personal data

Pursuant to Article 1 of the DP Law, personal data is defined as any information regardless of their nature, and format, relating to an identified or identifiable person.

Definition of sensitive personal data

Sensitive personal data is defined under the law as personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs or union membership of the person concerned or relating to his health, including his genetic data (article 1.3 of the DP Law).

NATIONAL DATA PROTECTION AUTHORITY

The relevant authority is the Data Protection National Commission (*Commission Nationale de Protection des Données Personnelles*).

REGISTRATION

The processing of personal data is subject:

- To a prior declaration to be filed with the Personal Data Protection Commission, and
- To the prior authorization of the Data Protection National Commission (*Commission Nationale de Protection des Données Personnelles*) when the processing concerns any of the following:
    - Sensitive data (*eg*, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, including genetic data)
    - Using personal data for purposes other than those for which they were initially collected
    - Genetic data, except for those used by health personnel and that respond to medical purposes
    - Data relating to offenses, convictions or security measures, except for those used by the officers of the court

- Data which includes the number of the national identity card of the concerned person

The declaration and authorization includes a commitment that the personal data will be treated in accordance with the DP Law.

The prior declaration and authorization shall include, without limitation, the following information:

- The name and address of the person in charge of the processing and, if applicable, its representative
- The name, characteristics and purpose(s) of the intended processing
- A description of the category or categories of data subjects, and the data or categories of personal data relating thereto
- The recipients or categories of recipients to whom the data are likely to be communicated
- The intended transfers of data to foreign states
- The data retention time
- The authority with which the data subject may exercise, if any, the rights granted to him / her by law, and the measures taken to facilitate the exercise of these rights
- A general description allowing a preliminary assessment of the appropriateness of the measures taken to ensure the confidentiality and security of processing, and
- Overlap, interconnections, or any other form of data reconciliation and their transfer, subcontracting, in any form, to third parties, free of charge or for consideration

DATA PROTECTION OFFICERS

There is no requirement for a data protection officer under the DP Law.

COLLECTION & PROCESSING

The personal data must be processed in accordance with the following principles:

- Treated fairly and lawfully
- Collected for specific, explicit and legitimate purposes
- Adequate, relevant and not excessive
- Accurate and necessary and kept up-to-date
- Kept in a form enabling the person concerned to be identified

As a general rule, the processing of a personal data must be subject to the prior consent of the relevant data subject.

However, the processing of personal data can be performed without the consent of the relevant data subject provided that the information relates to the:

- Compliance with a legal obligation to which the relevant data subject or the person in charge of the processing are submitted
- Execution of a contract to which the relevant data subject is party or in the performance of pre-contractual measures taken at the request of the latter
- Protection of the vital interests of the relevant data subject, if that person is physically or legally unable to give its consent

- Performance of a task of public interest or related to the exercise of public authority, vested in the person in charge of the processing or the third party to whom the data are communicated
- Fulfillment of the legitimate interests pursued by the person in charge of the processing or by the recipient, subject not to disregard the interests or fundamental rights and freedoms of the relevant data subject

TRANSFER

Prior authorization from the National Commission is required before any transfer of personal data to a foreign state.

Further, the person in charge of the processing operation can transfer personal data to a foreign state only if the said state ensures under its applicable legal framework an adequate level of protection for the privacy and fundamental rights and freedoms of individuals regarding the processing to which these data is or might be subject, unless:

- The data subject has expressly consented to the transfer
- The transfer and subsequent processing is required for:
    - Compliance with a legal obligation to which the concerned person or the person in charge of the processing are submitted
    - The execution of a contract to which the concerned person is party or in the performance of pre-contractual measures taken at the request of the latter
    - The protection of the vital interests of the relevant data subject, if that person is physically or legally unable to give its consent
    - Performance of a task of public interest or related to the exercise of public authority, vested in the person in charge of the processing or the third party to whom the data are communicated
    - Fulfillment of the legitimate interests pursued by the data controller or by the recipient, when not outweighed by the interests or fundamental rights and freedoms of the relevant data subject

In practice, we notice that CNDP interprets the exception of legitimate interests of the data processor very restrictively. CNDP is in general more comfortable relying on the data subject's consent regarding any transfers to a foreign state.

SECURITY

Article 23 of the DP Law provides that an organization is required to implement all technical and organizational measures to protect personal data in order to prevent it being damaged, altered or used by a third party who is not authorized to have access, as well as to protect it against any form of illicit processing.

Additionally, in appointing processors and subcontractors an organization must choose a processor or subcontractor who provides sufficient guarantees with regard to the technical and organizational measures relating to the processing to be carried out while ensuring compliance with these measures.

BREACH NOTIFICATION

There is no requirement for a data protection officer under the DP Law, except, where relevant, through the application of GDPR.

ENFORCEMENT

The Data Protection National Commission enforces compliance of the DP Law.

Article 50 to 64 provide that non-compliance with the DP Law is punishable by a fine ranging from DH10,000 to DH600,000 and / or imprisonment between three months and four years.

If the offender is a legal person, and without prejudice to the penalties which may be imposed on its officers, penalties of fines shall be doubled.

In addition, the legal person may be punished with one of the following penalties:

- The partial confiscation of its property
- Seizure of objects and things whose production, use, carrying, holding or selling is an offense
- The closure of the establishment(s) of the legal person where the offense was committed

ELECTRONIC MARKETING

Direct marketing by means of an automated calling machine, a fax machine, email or a similar technology, which uses, in any form whatsoever, an individuals' data without their express prior consent to receive direct prospecting is prohibited.

However, direct marketing via email may be allowed if the recipient's email address has been received directly from him / her.

In the absence of consent, unwanted emails can only be sent if all of the following conditions are satisfied:

- The contact details were provided in the course of a sale
- The marketing relates to a similar product
- The recipient was given a method to opt out of the use of their contact details for marketing when they were collected

ONLINE PRIVACY

The general data protection principles under the DP Law apply.

KEY CONTACTS

Christophe Bachelet
Partner
T +33 140 152 559
Christophe.Bachelet@dlapiper.com

Mehdi Kettani
Partner
Mehdi.Kettani@dlapiper.com

Kawtar Bedraoui Idrissi
Associate
T +212(0)520 42 78 33
kawtar.bedraoui@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MOZAMBIQUE

Last modified 28 January 2019

LAW

In Mozambique there is no specific legislation on data protection or privacy. However, there are other sources of law that impose some privacy obligations, including:

- The Civil Code (Decree-Law no. 47344, of November 25, 1966, in force in Mozambique through Edict no. 22869, dated September 4, 1967)
- The Penal Code (Law n.° 35/2014 of December 31)
- The Labour Law (Law n.° 23/2007, of August 1)
- The Electronic Transactions Law (Law n.° 3/2017, of January 9)

In addition, the Constitution of the Republic of Mozambique provides that all citizens are entitled to the protection of their private life and have the right to honor, good name, reputation, protection of their public image and privacy. Further, Article 71 of the Constitution identifies the need to legislate on access, generation, protection and use of computerized personal data (either by public or private entities); however, implementing legislation has not yet been approved.

DEFINITIONS

Definition of personal data

At the moment, the law does not define the concept of 'personal data'.

Definition of sensitive personal data

There is no law defining sensitive personal data. However, the Constitution of the Republic of Mozambique imposes restrictions on recording and handling any individually identifiable information concerning a person's political, philosophical or ideological beliefs, religious beliefs, membership in a political party or trade union and (particulars) related to the person's privacy.

NATIONAL DATA PROTECTION AUTHORITY

There is no data protection authority in Mozambique.

REGISTRATION

There is no data protection registration requirement in Mozambique.

DATA PROTECTION OFFICERS

Mozambique law does not require the appointment of data protection officers.

COLLECTION & PROCESSING

Under the Constitution of the Republic of Mozambique, individually identifiable information, concerning to political, philosophical or ideological beliefs, religious beliefs, membership in a political party or trade union and (particulars) related to the person's privacy may not be stored or processed in a database.

TRANSFER

The law does not generally restrict cross-border transfers of personal information. The Constitution of the Republic of Mozambique imposes restrictions on disclosures of personal information to third parties.

SECURITY

Under the Electronic Transactions Law (Law n.° 3/2017, of January 9), the person / entity responsible for processing electronic data, must protect personal data against risks, losses, unauthorized access, destruction, use, modification or disclosure.

BREACH NOTIFICATION

There is no breach notification requirement in Mozambique.

ENFORCEMENT

The Penal Code (Law n.° 35/2014 of December 31) provides for certain computer-related crimes, such as intrusion through informatics, which is subject to imprisonment from two to eight years and a one-year fine. There is also the crime of fraud through electronic means, which is subject to imprisonment for at least one year and a corresponding fine.

However, given that Mozambique does not have specific data protection laws nor a specific authority responsible to oversee data protection matters, enforcement of data protection-related matters is minimal.

ELECTRONIC MARKETING

The rules applicable to electronic advertisement and marketing are provided under the Advertisement Code (Decree n.° 38/2016, of August 31) and the Electronic Transactions Law (Law n.° 3/2017, of January 9).

Under the Electronic Transactions Law, express consent from a recipient is required prior to sending direct marketing communications via automated dialing systems, fax machines and email, unless one of the following applies:

- If the sender obtained the contact details of the recipient during the sale or negotiations for the sale of a product or service to the recipient
- The direct marketing refers to similar products or services to those of the recipient
- At the moment of initial collection of the data, the recipient was offered the option to refuse of use of his contact details, and decided not to refuse
- If the recipient did not refuse the use of its data in any subsequent communications

Under the Advertisement Code, electronic marketing messages should be clearly identified and include sufficient information, so as to allow the common recipient to easily understand all of the following:

- The nature of the message
- The advertiser
- The promotional offers, such as discounts, prizes, gifts and promotional contests and games, as well as the conditions to which they are bound (if applicable)

All direct marketing message must provide recipients with information about how to opt out of further marketing communications, as well as the identity details of the source from which the contact details of the consumer have been obtained.

ONLINE PRIVACY

Other than the above general rule, there are no other rules applicable to online privacy.

KEY CONTACTS

Eduardo Calu
Managing Partner
SAL & Caldeira Advogados, Lda.
T +258 21 241 400
ecalu@salcaldeira.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NAMIBIA

Last modified 23 May 2019

LAW

Namibia has not enacted comprehensive data privacy legislation. However, various sector-specific laws are in place to protect client information, including in the legal and banking sectors.

Namibia recognizes the right to privacy as a fundamental human right under Article 13 of the Namibian Constitution. Accordingly, all persons have a right to privacy in their homes and communications. The right to privacy is limited as required by law and in the interest of protecting:

- national security and public safety
- the nation's economy
- health and morals
- against disorder and crime
- the rights and freedoms of others

The Namibian Government is currently drafting a Data Protection Policy that, although not yet public, is expected to:

- protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to data processing
- protect Namibian citizens from abuse of their personal data, and
- harmonize Namibia's data protection policy and legal framework with regional and international standards to promote the free flow of personal data under conditions of assurance and trust

Further, the Ministry of Information and Communication Technology (MICT) is expected to finalize a draft Data Protection bill in 2019 or 2020.

DEFINITIONS

Definition of Personal Data

Not defined.

Definition of Sensitive Personal Data

Not defined.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in Namibia.

REGISTRATION

There is no registration requirement.

DATA PROTECTION OFFICERS

MICT

COLLECTION & PROCESSING

There are no restrictions on the collection and processing of personal data.

TRANSFER

There are no data transfer restrictions in place.

SECURITY

There are no data security requirements.

BREACH NOTIFICATION

There are no requirements to report data breaches to any individual or regulatory body.

ENFORCEMENT

There is no enforcement mechanism in place.

ELECTRONIC MARKETING

There are no electronic marketing regulations.

ONLINE PRIVACY

There are no specific laws that regulate the manner in which personal data may be stored or transmitted online.

KEY CONTACTS

Peter Johns
Director
Ellis Shilengudwa Incorporated
T +264 61 242224
peter@esinamibia.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NETHERLANDS

Last modified 10 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Dutch GDPR Implementation Act (*Uitvoeringswet AVG,* the **Implementation Act**) constitutes the local implementation of the GDPR in the Netherlands. The Implementation Act follows a policy-neutral approach, meaning that the requirements of the previous Dutch Data Protection Act (*Wet bescherming persoonsgegevens*) are maintained insofar as possible under the GDPR. The Implementation Act provides for, among other things, national rules where this is necessary for the implementation of GDPR provisions on the position of the regulatory authority or the fulfilment of discretionary powers provided by the GDPR.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions are largely the same as in Article 4, GDPR. In addition, the Implementation Act defines "personal data concerning criminal law matters" as personal data concerning criminal convictions and offences or related security measures as referred to in Article 10, GDPR, as well as personal data relating to a prohibition imposed by the courts for unlawful or objectionable conduct.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) has been appointed by law as the supervisory data protection authority and supervises compliance with the GDPR and the Implementation Act.

The Dutch Data Protection Authority's contact details are as follows:

Autoriteit Persoonsgegevens

Postbus 93374

2509 AJ DEN HAAG

Telephone number: (+31) - (0)70 - 888 85 00

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection laws and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Implementation Act (Article 39) provides more detailed information regarding the secrecy requirement set out in Article 38(5) GDPR, by stipulating that the DPO must maintain the secrecy of any information that becomes known to him or her pursuant to a complaint by or request from a data subject, unless the data subject agrees to disclosure.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to demonstrate compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity

- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this

- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision taking, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (*ie,* opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Special categories of personal data (Article 9)

Article 9(2) of the GDPR provides for a number of exceptions under which special categories of personal data may lawfully be processed. Certain of these exceptions require a basis in Member State law.

Division 3.1 of the Implementation Act provides for various exceptions for the processing of different types of special categories of personal data, subject to stringent conditions. Important examples include exceptions for:

- Scientific or historical research or statistical purposes
- The processing of personal data revealing racial or ethnic origin
- The processing of personal data revealing political opinions for the performance of public duties
- The processing of personal data revealing religious or philosophical beliefs for spiritual care
- Genetic, biometric and health data

Criminal convictions and offences data (Article 10)

The processing of criminal conviction or offences data is prohibited by Article 10 of the GDPR, except where specifically authorized under relevant Member State law.

Division 3.2 of the Implementation Act provides several exceptions for the processing of criminal convictions and offences data.

The following general grounds for exemptions for processing criminal convictions and offences data apply:

- Explicit consent by the data subject
- Protection of a data subject's vital interests
- Processing related to personal data manifestly made public by the data subject
- Processing necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity
- Processing necessary for reasons of substantial public interest
- Processing necessary for scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR, and the conditions referred to in Section 24(b) to (d) of the Implementation Act have been met

Specific exceptions may apply on the basis of Article 33 of the Implementation Act, *eg,* where the processing is carried out by bodies that are responsible pursuant to law for applying criminal law, or where the processing is necessary in order to assess a request from the data subject to take a decision on him or her or to provide a service to him or her.

Child's consent to information society services (Article 8)

The Netherlands did not make use of the option to provide for a lower age limit for the processing of personal data of a child on the basis of Article 8, GDPR.

Automated Decision Making (Article 22)

The Netherlands has made use of the possibility provided by Article 22(2)(b) GDPR, and has implemented exceptions from the prohibition on automated individual decision-making. Article 40 of the Implementation Act sets out that Article 22(1) of the GDPR does not apply if the automated individual decision-making, other than based on profiling, is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out for reasons of public interest. Examples provided by the Explanatory Memorandum to the Implementation Act concern situations where there may be automated individual decision making on the basis of strictly individual characteristics, *eg,* in the case of awarding certain allowances (*eg,* study allowances, child allowances), where there is no reason to require human intervention. In such cases, the controller must take suitable measures to safeguard the data subject's rights, freedoms and legitimate interests. Such suitable measures will in any case have been taken if the right to obtain human intervention, the data subject's right to express his or her point of view and the right to contest the decision, have been safeguarded.

Processing of national identification number (Article 87)

Article 87 of the GDPR sets out that Member States may further determine the specific conditions for the processing of a national identification number. The Netherlands has made use of this possibility: Article 46 of the Implementation Act sets out that a national identification number may only be processed where explicitly allowed by law, and only for those purposes stipulated by the relevant law.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
d. The transfer is necessary for important reasons of public interest
e. The transfer is necessary for the establishment, exercise or defence of legal claims
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
g. The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the

purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State. A transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

No specific local rules have been adopted on the basis of Articles 44-50, GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

The Netherlands has not implemented any specific regulations on the basis of Articles 24, 25 or 32 of the GDPR. In this respect, the Explanatory Memorandum to the Dutch Implementation Act explains that no general standard will be developed which sets out when an organization has fulfilled its technical and organizational security obligations. However, specific sectoral codes of conduct may be implemented which may contain further concrete standards. For example, in the health sector we see that such security standards already exist (*eg,* NEN 7510, which applies as an important information security standard in the health sector).

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The provisions regarding data breach notifications are mostly identical to Articles 33 and 34 GDPR.

Data breaches that require notification, should be notified to the Dutch DPA by completing an online form through the Dutch DPA website.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define undertaking and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of undertaking. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called look through liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- Data subjects' rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered material or non-material damage as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of non-material damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

On the basis of Article 58(6) GDPR and in addition to the power to impose fines pursuant to the GDPR, the Dutch DPA has the power to impose an administrative enforcement order (*last onder bestuursdwang*) or an order subject to penalty (*last onder dwangsom*) to enforce obligations laid down by or pursuant to the Implementation Act.

ELECTRONIC MARKETING

The GDPR applies to most electronic marketing activities, as these will involve some use of personal data (*eg,* an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Electronic marketing is partially regulated in Article 11.7 of the Dutch Telecommunications Act (Tw). In the context of this Article electronic marketing could be defined as SMS, email, fax and similar media for the purposes of unsolicited communication related to commercial, charitable or ideal purposes without the individuals' prior express consent.

Electronic marketing directed to corporations does not require prior consent if:

- The advertiser or electronic marketer uses electronic address data intended for this particular purpose, and
- If the individual is located outside the EU, the advertiser or electronic marketer complies with the relevant rules of that particular country in this respect

On the basis of Article 11.7 of the Tw, electronic marketing to individuals is in principle prohibited. If certain conditions are being met, such as prior express consent, electronic marketing directly to individuals can be allowed. Furthermore, electronic marketing to individuals is also allowed if it is restricted to the marketing of existing customers and restricted to similar products or services of the advertiser or electronic marketer. In the latter case, the advertiser or electronic marketer is obligated to provide opt-out possibilities to customers when obtaining data from customers and in every marketing message sent.

ONLINE PRIVACY

Traffic Data

Traffic Data is regulated in Article 11.5 of the Tw. Traffic Data held by a public electronic communications services provider (CSP) must be erased or anonymized when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- It is being used to provide a value added service, and
- Consent has been given for the retention of the Traffic Data.

Traffic Data can only be processed by a CSP for:

- The management of billing or traffic
- Dealing with customer enquiries
- The prevention of fraud
- The provision of a value added service (subject to consent)
- Market research (subject to consent)

Location Data

(Traffic Data not included) – Location Data is regulated in Article 11.5a of the Tw. Location Data may only be processed:

- If such data is being processed in anonymous form; or
- With informed consent of the individual.

Cookie Compliance

The Netherlands implemented the E-Privacy Directive through the Dutch Telecommunications Act in Article 11.7a. The Authority for Consumers and Markets (ACM) is entrusted with the enforcement of Article 11.7a of the Tw.

The main rule is that the website operator needs to obtain prior consent from a user before using cookies (opt-in) and needs to clearly and unambiguously inform the user about these cookies (purpose, type of cookie, etc). Implicit consent is accepted under the current Dutch regime, however it is unclear whether this will be upheld after the ePrivacy Regulation will come into force. Please note that the website operator is entitled to refuse users access to its website(s) if no consent is given. The requirement to obtain prior consent from a user does not apply in case of functional cookies that have little or no impact on the user's privacy (*eg,* first party cookies).

The use of analytic cookies, affiliate or performance cookies used for the purpose of paying affiliates or cookies used for testing the effectiveness of certain banners will be allowed without consent, on the condition that:

- The data collected by such cookies are not used for, among other things, creating profiles by the website owner or third parties with whom the data are shared, and
- Website owners sharing the data with a third party take additional measures in order to limit any possible privacy impact.

The information collected through cookies are considered personal data, unless the party that places the cookies can prove

otherwise. This applies only to tracking cookies, where the surfing behavior of customers on several different websites is being observed (and the information obtained is being used for commercial purposes).

In case of violation of electronic marketing or online privacy legislation, the ACM can impose fines of up to EUR 900,000 per violation.

KEY CONTACTS

Richard van Schaik
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +31 20 541 9828
richard.vanschaik@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NEW ZEALAND

Last modified 28 January 2019

LAW

The Privacy Act 1993 (Act) governs how agencies collect, use, disclose, store, retain and give access to personal information. The Act gives the Privacy Commissioner the power to issue codes of practice that modify the operation of the Act in relation to specific industries, agencies, activities or types of personal information. The following codes are currently in place:

- Credit Reporting Privacy Code
- Health Information Privacy Code
- Justice Sector Unique Identifier Code
- Superannuation Schemes Unique Identifier Code
- Telecommunications Information Privacy Code
- Civil Defence National Emergencies (Information Sharing) Code

Enforcement is through the Privacy Commissioner.

A Privacy Amendment Bill was introduced to New Zealand's parliament in 2018. If enacted it will include stronger powers for the Privacy Commissioner, mandatory reporting of privacy breaches, new offenses and increased fines. Timing and final content are not yet known, but the bill is expected to become law during 2019. The Privacy Commissioner has requested further amendments to the bill.

DEFINITIONS

Definition of personal data

Personal information under the Act is defined as information about an identifiable individual and includes information relating to a death that is maintained by the Registrar General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act.

Definition of sensitive personal data

Although no differentiation is made between how different types of personal information are to be treated under the Act, the codes of practice issued by the Privacy Commissioner may modify the operation of the Act for specific industries, agencies, activities and types of personnel information.

Definition of agency

Agency is defined under the Act as any person or body of persons, whether corporate or unincorporated, and whether in the public sector (including government departments) or the private sector. Certain bodies are specifically excluded from the definition.

NATIONAL DATA PROTECTION AUTHORITY

The Privacy Commissioner's Office

Level 4
109-111 Featherston Street
Wellington 6143
New Zealand

T +64 474 7590
F +64 474 7595

enquiries@privacy.org.nz
www.privacy.org.nz

REGISTRATION

There is no obligation on agencies to notify the Privacy Commissioner that they are processing personal information. However, the Privacy Commissioner may require an agency to supply information for the purpose of publishing or supplementing a directory or to enable the Privacy Commissioner to respond to public enquiries in this regard.

The Privacy Commissioner may from time to time publish a directory of personal information processing activities including the following:

- The nature of any personal information held by an agency
- The purpose for which personal information is held by an agency
- The classes of individuals about whom personal information is held by an agency
- The period for which personal information is held by an agency
- The individuals entitled to access personal information held by an agency and the conditions relating to such access
- Steps to be taken by an individual wishing to obtain access to personal information held by an agency

DATA PROTECTION OFFICERS

The Act requires each agency to appoint within that agency, one or more individuals to be a privacy officer. The privacy officer's responsibilities include the following:

- The encouragement of compliance with the personal information privacy principles contained in the Act
- Dealing with requests made to the agency pursuant to the Act
- Working with the Privacy Commissioner in relation to investigations relating to the agency
- Ensuring compliance with the provisions of the Act

Provided the person appointed a privacy officer is within the agency, that person does not have to be a New Zealand citizen or reside in New Zealand.

Failure to appoint a privacy officer or obstructing or hindering the Privacy Commissioner is an offense under the Act.

COLLECTION & PROCESSING

Subject to specific exceptions, agencies may collect, store and process personal information in accordance with the following 12 information privacy principles:

- The personal information is needed for a lawful purpose connected with the agency's work
- The personal information is collected directly from the relevant person (unless a relevant exception applies as set forth below)
- Before the personal information is collected, the agency has taken reasonable steps to ensure that the person knows that the information is being collected; the purpose for which it is being collected; the intended recipients; the name and address of the agency collecting and holding the information; if the information is authorized or required by law, the applicable law and the consequences if the requested information is not provided; and that the person concerned may access and correct the information
- The personal information is not collected in an unlawful or unfair way or in a way that unreasonably invades a person's privacy
- The personal information must be kept reasonably safe from being lost, accessed, used, modified or disclosed to unauthorized persons
- If the personal information is readily retrievable, the relevant person is entitled to know whether information is held and to have access to it
- The relevant person is entitled to request correction of the personal information. If the agency will not correct the information, the person may provide a statement of the correction sought to be attached to the personal information
- Before it is used, the agency must ensure that the personal information is accurate, up-to-date, complete, relevant and not misleading
- The personal information may not be kept for any longer than it is needed
- Subject to certain exceptions, personal information collected for one purpose may not be used for another purpose
- An agency must not disclose personal information to another person, body or agency except in specific circumstances
- An agency may only assign a unique identifier to an individual if it is needed for the agency to carry on its work efficiently and may not assign a unique identifier to an individual if the same identifier is used by another agency

Personal information does not need to be collected directly from the relevant person if:

- The personal information is publicly available
- The relevant person authorizes collection of the personal information from someone else
- Non-compliance would not prejudice the interests of the relevant individual
- The personal information is being collected for a criminal investigation, enforcement of a financial penalty, protection of public revenue or the conduct of court proceedings
- Compliance would prejudice the purpose of the collection of the personal information or is not practical in the circumstances
- The personal information will be used in a way which will not identify the person concerned

TRANSFER

An agency should not disclose personal information to another entity unless the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which

the information was obtained. Care must be taken that all safety and security precautions are met to ensure the safeguarding of that personal information to make certain that it is not misused or disclosed to any other party.

The Privacy Commissioner is given the power to prohibit a transfer of personal information from New Zealand to another state, territory, province or other part of a country (State) by issuing a transfer prohibition notice (Notice) if it is satisfied that information has been received in New Zealand from one State and will be transferred by an agency to a third State which does not provide comparable safeguards to the Act and the transfer would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the Organisation for Economic Co-operation and Development (OECD) Guidelines, which include:

- The collection limitation principle (there should be limits to the collection of personal data)
- The data quality principle (personal data should be accurate, complete and kept up to date)
- The purpose specification principle (the purposes for which personal data are collected should be specified)
- The use limitation principle (personal data should not be used otherwise than in accordance with the purpose specification principle, except with the consent of the data subject or by authority of law)
- The security safeguards principle (personal data should be protected by reasonable security safeguards)
- The openness principle (there should be a general policy of openness about developments, practices and policies relating to personal data)
- The individual participation principle (individuals should have the right to obtain confirmation of whether a data controller holds their personal data, to have that data communicated to him/her, to be given reasons if a request for that data is denied and to be able to challenge that denial, and to challenge data relating to him/her and have that data erased, rectified, completed or amended if successful)
- The accountability principle (a data controller should be accountable for complying with the above principles)

In considering whether to issue a Notice, the Privacy Commissioner must have regard to whether the proposed transfer of personal information affects, or would be likely to affect any individual, the desirability of facilitating the free flow of information between New Zealand and other States, and any existing or developing international guidelines relevant to trans-border data flows.

On December 19, 2012 the European Commission issued a decision formally declaring that New Zealand law provides a standard of data protection that is adequate for the purposes of EU law. This decision means that personal data can flow from the 27 EU member states to New Zealand for processing without any further safeguards being necessary.

Following the decision in the Schrems case, where the European Commission's decision to recognize the safe harbor agreement with the USA was invalidated, there have been calls to review New Zealand's adequacy status, primarily due to New Zealand's membership with the Five Eyes network. However, to date this has not been acted upon by the European Commission.

SECURITY

An agency that holds personal information shall ensure that the information is kept securely and protected by such security safeguards as are reasonable in the circumstances to protect against:

- Loss
- Access, use, modification or disclosure, except with the authority of the agency
- Other misuse or unauthorized disclosure

If it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency must be done to prevent unauthorized use or unauthorized disclosure of the information.

BREACH NOTIFICATION

There is no mandatory requirement in the Act to report an interference with privacy. There will be a mandatory requirement to report data breaches once the Privacy Amendment Bill is enacted, which is expected to occur during 2019.

Any person may make a complaint to the Privacy Commissioner alleging an action is, or appears to be, an interference with the privacy of an individual. For there to be an interference with privacy, there must be a breach of the law and the breach must lead to financial loss or other injury, an adverse effect on a person's right, benefit, privilege, obligation or interest or significant humiliation, loss of dignity or injury to a person's feelings. There is no requirement to show harm in a complaint about access to, or correction of, personal information. An unauthorized disclosure of personal information is sufficient to breach the Act.

ENFORCEMENT

In New Zealand, the Privacy Commissioner is responsible for investigating a breach of privacy laws. The Privacy Commissioner has powers to enquire into any matter if the Privacy Commissioner believes that the privacy of an individual is being, or is likely to be, infringed. The Privacy Commissioner will primarily seek to settle a complaint by conciliation and mediation. If a complaint cannot be settled in this way, a formal investigation may be conducted so that the Privacy Commissioner may form an opinion on how the law applies to the complaint. The Privacy Commissioner's opinion is not legally binding but is highly persuasive. The Privacy Commissioner is not able to issue a formal ruling or determination and cannot begin prosecution proceedings or impose a fine.

If the Privacy Commissioner is of the opinion that there has been an interference with privacy, the Privacy Commissioner may refer the matter to the Director of Human Rights who may then in turn decide to take the complaint to the Human Rights Review Tribunal. The Tribunal will hear the complaint afresh and its decision is legally binding. It can award damages for breaches of privacy.

ELECTRONIC MARKETING

The Act does not differentiate between the collection of and use of any personal information for electronic marketing or other forms of direct marketing.

The Unsolicited Electronic Messages Act 2007:

- Prohibits unsolicited commercial electronic messages (this includes email, fax, instant messaging, mobile / smart phone text (TXT) and image-based messages of a commercial nature – but does not cover Internet pop-ups or voice telemarketing) with a New Zealand link (messages sent to, from or within New Zealand)
- Requires commercial electronic messages to include accurate information about who authorized the message to be sent
- Requires a functional unsubscribe facility to be included so that the recipient can instruct the sender not to send the recipient further messages
- Prohibits using address-harvesting software to create address lists for sending unsolicited commercial electronic messages

The Marketing Association of New Zealand has a code of practice for direct marketing which governs compliance by members of the principles of the code. The code establishes a 'Do Not Call' register to which anyone not wanting to receive any direct marketing can register.

ONLINE PRIVACY

Other than compliance with the Act, no additional legislation deals with the collection of location and traffic data by public electronic communications services providers and use of cookies (and similar technologies). The New Zealand Privacy

Commissioner has general guidelines on protecting online privacy.

KEY CONTACTS

DLA Piper New Zealand
www.dlapiper.co.nz/

John Hannan
Partner
T +64 9 399 3843
john.hannan@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NIGERIA

Last modified 20 May 2019

LAW

Nigeria has not enacted comprehensive data privacy and protection legislation. However, various pending and enacted sector-specific laws contain privacy and data protection provisions.

THE LAWS

Constitution of the Federal Republic of Nigeria 1999 (As Amended)

The Nigerian Constitution provides Nigerian citizens with a fundamental right to privacy. Section 37 of the Constitution guarantees privacy protections to citizens in their homes, correspondence, telephone conversations and telegraphic communications. The Constitution does not define the scope of "privacy" or contain detailed privacy provisions.

Child Rights Act 2003

This Child Rights Act 2003 reiterates the constitutional right to privacy as relates to children. Section 8 of the Act guarantees a child's right to privacy subject to parent or guardian rights to exercise supervision and control of their child's conduct. Some Nigerian states have also enacted Child Rights Laws.

Consumer Code of Practice Regulations 2007 (NCC Regulations)

The Nigerian Communications Commission (NCC) issued the NCC Regulations to require all licensees to take reasonable steps to protect customer information against improper or accidental disclosure, and ensure that such information is securely stored and not kept longer than necessary. The NCC Regulations further prohibit the transfer of customer information to any party except to the extent agreed with the Customer, as permitted or required by the NCC or other applicable laws or regulations.

Consumer Protection Framework 2016 (Framework)

The Consumer Protection Framework 2016 was enacted pursuant to the Central Bank of Nigeria Act 2007. The Framework contains provisions that prohibit financial institutions from disclosing customers personal information. The Framework further requires that financial institutions have appropriate data protection measures and staff training programs in place to prevent unauthorized access, alteration, disclosure, accidental loss or destruction of customer data. Financial services providers must obtain written consent from consumers before personal data is shared with a third party or used for promotional offers.

Credit Reporting Act 2017

The Credit Reporting Act establishes a legal and regulatory framework for credit reporting by Credit Bureaus. Section 5 of the Credit Reporting Act requires Credit Bureaus to maintain credit information for at least 6 years from the date that such information is obtained, after which the information must be archived for a 10-year period prior to its destruction. Section 9 of the Credit Reporting Act provides the rights of data subjects (i.e. persons whose credit data are held by a credit bureau) to

privacy, confidentiality and protection of their credit information. Section 9 further prescribes conditions where data subject credit information may be disclosed.

Cybercrimes (Prohibition, Prevention Etc) Act 2015

The Cybercrimes (Prohibition, Prevention Etc) Act provides a legal and regulatory framework that prohibits, prevents, detects, prosecutes and punishes cybercrimes in Nigeria. The Act requires financial institutions to retain and protect data and criminalizes the interception of electronic communications.

Freedom of Information Act, 2011 (FOI Act)

The FOI Act seeks to protect personal privacy. Section 14 of the FOI Act provides that a public institution is obliged to deny an application for information that contains personal information unless the individual involved consents to the disclosure, or where such information is publicly available. Section 16 of the FOI Act provides that a public institution may deny an application for disclosure of information that is subject to various forms of professional privilege conferred by law (such as lawyer-client privilege, health workers-client privilege, etc.).

National Identity Management Commission (NIMC) Act 2007

The NIMC Act creates the NIMC to establish and manage a National Identity Management System (NIMS). The NIMC is responsible for enrolling citizens and legal residents, creating and operating a National Identity Database and issuing Unique National Identification Numbers to qualified citizens and legal residents. Section 26 of the NIMC Act provides that no person or corporate body shall have access to data or information contained in the Database with respect to a registered individual without authorization from the Commission. The Commission is empowered to provide a third party with information recorded in an individual's Database entry without the individual's consent, provided it is in the interest of National Security.

National Health Act 2014 (NHA)

The NHA provides rights and obligations for health users and healthcare personnel. Under the NHA, health establishments are required to maintain health records for every user of health services and maintain the confidentiality of such records. The NHA further imposes restrictions on the disclosure of user information, and requires persons in charge of health establishments to set up control measures for preventing unauthorized access to information. The NHA applies to all information relating to patient health status, treatment, admittance into a health establishment, and further applies to DNA samples collected by a health establishment.

Nigerian Communications Commission (registration of telephone subscribers) Regulation 2011

Section 9 and 10 of the Nigerian Communications Commission Regulation 2011 provides confidentiality for telephone subscriber records maintained in the NCC's central database. The Regulation further provides telephone subscribers with a right to view and update personal information held in the NCC's central database of a telecommunication company.

Nigeria Data Protection Regulation

The National Information Technology Development Agency (NITDA) was established under the NITDA Act, 2007 as the national authority for planning, developing and promoting the use of information technology in Nigeria. The NITDA issued the Nigeria Data Protection Regulation (Regulation) in January 2019, to regulate and control the use of data in Nigeria. The Regulation mandates all public and private organizations in Nigeria that control data of natural persons to make available to the general public their respective data protection Policies within 3 months after the date of the issuance of the Regulation. These Policies must be in conformity with the Regulation.

Federal Competition and Consumer Protection Act, 2019

The Federal Competition and Consumer Act 2019 was enacted on February 6, 2019. Section 34(6) of the Act requires the Commission to protect the business secrets of all parties involved in Commission investigations. Section 33(2) requires Commission hearings to take place in public, but the Commission may, particularly to preserve business secrets, conduct hearings

in camera.

DEFINITIONS

Definition of personal data

Personal Data is defined as any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data is a broad term, encompassing anything from a name, address, photo, email address, bank details, social networking website posts, medical information, and other unique identifier such as, but not limited to, MAC address, IP address, IMEI number, IMSI number, SIM and others.

Definition of sensitive personal data

Sensitive Personal Data means data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.

Definition of data subject

Data Subject means an identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.

Definition of data controller

Data Controller means a person who either alone, jointly or in common with other persons, or as a statutory body, determines the purposes for and manner in which Personal Data is processed or is to be processed.

Definition of personal data breach

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Definition of processing

Processing means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

NATIONAL DATA PROTECTION AUTHORITY

There is no specific authority bestowed with the responsibility of the protection of data, however sector specific regulatory agencies including NITDA and NCC provide services relating to the protection of data.

REGISTRATION

There is no requirement to register databases.

DATA PROTECTION OFFICERS

The Regulations require Data Controllers to designate a Data Protection Officer responsible for ensuring compliance with the Regulations and other applicable data protection directives. The data controller may outsource this responsibility to a verifiably

competent firm or person.

COLLECTION & PROCESSING

COLLECTION

Personal Data must be collected and processed in accordance with a specific, legitimate and lawful purpose consented to by the Data Subject.

- Prior to Personal Data collection, Controllers must provide Data Subjects with relevant information, including the identity and contact details of the Controller, contact details of its Data Protection Officer and the intended purpose and legal basis for Personal Data processing.
- The legitimate interests pursued by the Controller or third party must be stated.
- The recipients or categories of recipients of the Personal Data, if any.
- Where applicable, the fact that the Controller intends to transfer Personal Data to a third country or international organization, and the existence or absence of an adequacy decision by the Agency, the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period.
- Data subjects must be provided with notice of their right to (a) request access to and rectification of Personal Data maintained by the Controller, (b) withdraw consent for further processing by the Controller at any time, and (c) lodge a complaint with the relevant authority.
- Where the Controller intends to process Personal Data for a purpose other than for which it was collected, the controller must provide Data Subjects with any relevant information on the additional purpose prior to further processing.

PROCESSING

Personal Data Processing is lawful if at least one of the following applies:

- The data subject has given consent to the processing of his or her Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official public mandate vested in the controller.
- Data processing by a third party shall be governed by a written contract between the third party and the Data Controller. Accordingly, any person engaging a third party to process the data obtained from Data Subjects shall ensure compliance with the Regulation.

TRANSFER

The Regulations include provisions on Personal Data transfers to foreign countries and international organizations, provided such transfers are intended for processing purposes. The Honorable Attorney General of the Federation (HAGF) is responsible for supervising such Personal Data transfers.

Personal Data transfers are permitted where the NITDA determines that a foreign country, territory or specific sector(s) within a foreign country or international organization provide adequate levels of Personal Data protection. The determination is based on the HAGF's consideration of the foreign country's legal system, rule of law, respect for human rights and fundamental freedoms, as well as relevant general and sector-specific legislation in public security, defense, national security and criminal law.

Personal Data transfers may take place without NITDA or HAGF authorization if:

- Data Subject expressly consents to the proposed transfer after being informed of associated risks in the absence of an adequacy determination, the lack of appropriate safeguards, and that there are no alternatives.
- Transfer is necessary for the performance of a contract between the Data Subject and the Controller or the

implementation of pre-contractual measures taken at the Data Subject's request.

- Transfer is necessary for the performance of a contract in the interests of the Data Subject between the Controller and another natural or legal person.
- Transfer is necessary for important reasons of public interest.
- Transfer is necessary for the establishment, exercise or defense of legal claims.
- Transfer is necessary to protect the vital interests of the Data Subject or of other persons, where the data subject is physically or legally incapable of giving consent.

Where Personal Data is transferred to a foreign country or to an international organization, the Data Subject shall have the right to be informed of the appropriate safeguards for data protection in the foreign country.

SECURITY

Anyone involved in data processing or the control of data has the responsibility to develop security measures to protect data. Such measures include but are not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organizational policies for handling Personal Data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff.

BREACH NOTIFICATION

There is no mandatory requirement to report data security breaches or losses to authorities or data subjects.

ENFORCEMENT

A breach of the Regulations is construed as a breach of the NITDA 2007. The NITDA enforces the NITDA Act 2007 by registering and licensing Data Protection Compliance Organizations to monitor, audit, train, and consult Data Controllers on compliance with the Regulations. Any licensee that contravenes the provisions of the Regulations is in breach and may be liable for penalties as determined by the Commission from time-to-time.

NITDA is mandated to set up an administrative redress panel to do the following:

- Investigate alleged violations of the Regulations
- Invite parties to respond to any allegations made against them within seven days
- Issue administrative orders to protect the subject matter of the allegation pending the outcome of investigation
- Conclude investigations and determine of appropriate redress within 28 working days.

ELECTRONIC MARKETING

The NCC Regulations provide that no licensee shall engage in unsolicited telemarketing unless it discloses:

- At the beginning of the communication, the identity of the licensee or other person on whose behalf it is made and the precise purpose of the communication
- During the communication, the full price of any product or service that is the subject of the communication
- That the person receiving the communication shall have an absolute right to cancel the agreement for purchase, lease or other supply of any product or service within seven (7) days of the communication, by calling a specific telephone number (without any charge, and that the Licensee shall specifically identify during the communication) unless the product or service has by that time been supplied to and used by the person receiving the communication

Licensees are required to conduct telemarketing in accordance with any "call" or "do not call' preferences recorded by the Consumer, at the time of entering into a contract for services or after, and in accordance with any other rules or guidelines issued by the Commission or any other competent authority.

Internet Service Providers (ISP)

The NCC Legal Guidelines for Internet Service Providers (ISP) provides that Commercial Communications ISPs must take reasonable steps to promote compliance with the following requirements for commercial email or other commercial communications transmitted using the ISP's services:

- The communication must be clearly identified as a commercial communication.
- The person or entity on whose behalf the communication is being sent must be clearly identified.
- The conditions to be fulfilled in order to qualify for any promotional offers, including discounts, rebates or gifts, must be clearly stated.
- Promotional contests or games must be identified as such, and the rules and conditions to participate must be clearly stated.
- Persons transmitting unsolicited commercial communications must take account of any written requests from recipients to be removed from mailing lists, including by means of public "opt-out registers" in which people who wish to avoid unsolicited commercial communications are identified.

Advertising

The Nigerian Code of Advertising Practice Sales Promotion and other rights and restrictions on practice provide that all advertisements and marketing communications directed at the Nigerian market using the Internet or other electronic media must comply with the following requirements:

- The commercial nature of such communications must not be concealed or misleading, it should be made clear in the subject header.
- Terms of the offer should be clear and devices should not be used to conceal or obscure any material factors, such as price or other sales conditions likely to influence customer decisions.
- The procedure for concluding a contract should be clear.
- Due recognition must be given to the standards of acceptable commercial behavior held by public groups before posting marketing communications to such groups using electronic media.
- Unsolicited messages should not be sent except where there are reasonable grounds to believe that consumers who receive such communications are interested in the subject matter or offer.
- All marketing communications sent via electronic media should include a clear and transparent mechanism enabling consumers to expressly opt-out from future solicitations.
- Care should be taken to ensure that neither the marketing communication, or applications used to enable consumers to open marketing or advertising messages, interfere with consumers normal use of electronic media.
- Customer information must not be transferred to any party except to the extent agreed with the Customer, as permitted or required by the NCC or other applicable laws or regulations.

ONLINE PRIVACY

The Constitutional right to privacy applies to electronic media, including mobile devices and the Internet. Violations of these rights may be subject to civil enforcement.

The NITDA Regulations require all mediums through which Personal Data is collected or processed to display a simple and conspicuous privacy policy, easily understood by the targeted Data Subject class. The privacy policy must contain the following, in addition to any other relevant information:

- What constitutes Data Subject consent
- Description of Personal Data to be collected
- Purpose of Personal Data collection

- Technical methods used to collect and store personal information (*ie*, cookies, web tokens, etc.)
- Access (if any) of third parties to Personal Data and purpose of access
- An overview of data processing principles under the Regulations
- Available remedies for privacy policy violations
- Timeframes associated with available remedies
- Any limitation clause, provided that no limitation clause shall avail any Data Controller who acts in breach of the principles of lawful processing set out in the Regulations

KEY CONTACTS

Olajide Oyewole LLP
www.olajideoyewole.com/

Sandra Oyewole
Partner
Olajide Oyewole LLP
T +234 1 279 3674
soyewole@olajideoyewole.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NORTH MACEDONIA

Last modified 28 January 2019

LAW

The Republic of North Macedonia (North Macedonia) regulates personal data protection issues under the Law on Personal Data Protection (Official Gazette of the Republic of Macedonia, nos. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015, 99/2016 and 65/2018) (DP Law), effective February 2005, amended March 2014. The DP Law is entirely harmonized with EC Directive 95/46/EC (Data Protection Directive).

North Macedonia expects to adopt a new data protection law in 2019 to align with the EU General Data Protection Regulation (GDPR).

DEFINITIONS

Defenition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable natural entity, where an identifiable entity is an entity whose identity can be especially determined, directly or indirectly, on the basis of his or her personal identification number or on one or a combination of features that are specific to his or her physical, mental, economic, cultural or social identity.

Defenition of sensitive personal data

Under the DP Law, sensitive personal data is personal data related to:

- Racial or ethnic origin
- Political or religious views, or other beliefs
- Membership in a trade union
- Health, including genetic data, biometric data and data referring to sexual life

NATIONAL DATA PROTECTION AUTHORITY

The Directorate for Personal Data Protection (DPA) was established in 2005 as North Macedonia's data protection authority. The DPA is an independent state agency with competence to oversee DP Law implementation, with its registered seat located at:

Bulevar Goce Delcev 8
Skopje
www.dlzp.mk

REGISTRATION

Any natural or legal entity who intends to collect, process or maintain a database containing personal data (Database) in North

Macedonia must notify the DPA prior to the commencement of any such activity.

This requirement does not apply to entities that:

- Have fewer than 10 employees
- Intend to process publicly available personal data
- Intend to process personal data of members of nonprofit organizations that are established for political, philosophical, religious or trade-union purposes

Entities must register (1) themselves as data controllers, and (2) their respective Databases with the DPA's Central Register of Databases. Data controllers must provide all relevant information on particular data processing activities, including: corporate details, types of data processed, purpose of processing, data retention periods, legal grounds for Database establishment, personal data transfers to other countries, and security measures in place to protect data integrity.

To register, entities must complete an online form: www.dzlp.mk. The DPA requires entities to report subsequent changes to registration details within 30 days of a change.

DATA PROTECTION OFFICERS

Under the DP Law, data controllers subject to registration requirements (see Registration section above) must appoint a data protection officer tasked with ensuring data controller compliance with the DP Law and other applicable regulations.

Data protection officers must:

- Participate in all decisions related to personal data processing and data subject rights over their personal data
- Prepare corporate by-laws on personal data protection, including technical and organizational measures designed to protect personal data and maintain its confidentiality
- Monitor data controller compliance with the DP Law and related regulations, specifically as relates to the corporate by-laws on personal data protection
- Coordinate internal personal data protection procedures and guidelines, and
- Develop data controller employee training on personal data protection

COLLECTION & PROCESSING

The DP Law sets forth the fundamental principles for personal data collection and processing require, which require that data controllers collect and process personal data:

- Fairly and lawfully
- For legitimate purposes
- Proportionally to the needs for collection and processing
- Accurately and completely, and
- To store data in a manner that enables data subject identification

Data controllers must obtain data subjects informed consent prior to personal data collection or processing, including as relates to personal identification numbers and sensitive personal data. Informed consent requires data controllers provide data subjects with all relevant information on personal data processing and collection, such as the purpose of processing, data subject rights, retention policy, and data transfers.

Exceptions to informed consent requirements permit data controllers to collect and process personal data without data subject consent to protect data subject life or vital interests, to protect public interests or to exercise the legitimate rights of the data controller, unless such processing or collection is in conflict with data subject fundamental rights and freedoms.

TRANSFER

Entities may only transfer personal data outside of North Macedonia to countries where adequate personal data protection levels apply. The DPA has authority to assess third country personal data protection levels and approve personal data transfers outside of North Macedonia.

Entities are not required to obtain DPA approval for personal data transfers to European Union (EU) and European Economic Area (EEA) countries, as the DP Law creates a legal assumption that EU and EEA countries provide adequate personal data protection levels.

Entities must obtain DPA approval for transfers to non-EU/EEA countries "white-listed" by the EC as providing adequate data protection levels, though through a simplified DPA approval process. The DPA relies on European Commission (EC) assessments of non-EU/EEA country personal data protection levels.

Personal data transfers outside of North Macedonia are prohibited, without the consent of the DPA, to third countries that the EC has not found to provide adequate data protection levels. Absent an EC adequacy determination, the DPA is required to assess and approve personal data transfers to non-EU/EEA countries. Minimal guidance exists on the DPA assessment and approval approach. Under the DP Law, DPA assessments should consider:

- The nature of the data
- The purpose and duration of the proposed processing
- Governing law in the country where the data is to be transferred, and
- Protective measures existing in the respective country

1: Andorra, Argentina, Australia, Canada (commercial organisations), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay and the US (only companies that are compliant with the Department of Commerce's Safe Harbour Privacy Principles).

SECURITY

The DP Law requires data controllers and processors to implement appropriate technical and organizational measures to protect personal data from accidental or illegal damage, illegal processing, accidental loss, change, unauthorized access or disclosure, and particularly as relates to processing that includes data transmission over a network. However, the DP Law does not require use of a specific technology to protect personal data.

Technical and organizational measures should be proportional to the risk posed by a breach to the integrity of data, considering the nature of the data being processed. The DP Law provides guidance to establish three personal data protection levels by using a combination of technical and organizational measures:

1. Basic
2. Medium
3. High

Data controllers and processors are required to adopt internal regulations (*ie*, corporate by-laws) with a description of technical and organizational measures for personal data protection.

BREACH NOTIFICATION

Under the DP Law, data controllers and processors are not required to report data security breaches to the DPA. The DPA is unable to trace data security breaches unless a data subject reports a breach of his or her rights, or through a random inspection of a data controller and processor.

ENFORCEMENT

The DPA has DP Law enforcement and oversight authority, and may monitor DP Law compliance through random data controller and processor inspections, or upon receipt of a data subject complaint.

The DPA enforces DP Law violations by ordering data controllers or processors to remedy violations within a specified time period, or by imposing a fine, taking the seriousness of the offense into consideration. Legal entity fines range from €1,000 to €2,000 per violation. Additionally, the DPA may issue a fine to the responsible person within the legal entity in an amount equal to 30% of the fine imposed on the legal entity. Entities may dispute DPA fines by initiating proceedings before the Administrative Court.

The DPA may further require data controllers or processors in violation of the DP Law to attend mandatory training on data protection issues organized by the DPA.

The Macedonian Criminal Code includes a criminal offense for misuse of personal data punishable by a monetary fine or imprisonment of up to one year, as determined by the court.

ELECTRONIC MARKETING

Under the DP Law, personal data may be processed for electronic marketing purposes only with the data subject explicit consent to such processing, provided that the data subject is entitled to withdraw his or her consent at any time free of charge.

ONLINE PRIVACY

There are no specific regulations governing online privacy, including cookies. However, general data protection rules under the DP Law apply to the extent possible.

KEY CONTACTS

Ljupka Noveska Andonova
Senior Associate
Karanovic & Partners
T +389 2 3223 870
ljupka.noveska@karanovicpartners.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NORWAY

Last modified 15 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The GDPR was incorporated in the EEA Agreement by a Joint Committee Decision dated July 6, 2018. The new Norweigan Personal Data Act ("PDA") implements GDPR and became effective as of July 20, 2018.

In addition to implementing GDPR, the PDA includes specific regulations as described below. In connection with the implementation of GDPR, several sector-specific regulations *eg,* in the healthcare sector has been updated to ensure compliance with GDPR.

The PDA has a similar geographical scope as GDPR article 3., *ie,*

1) data controllers and processors *established* in Norway regardless of whether the processing activities takes place Norway / EEA or not;

2) processing activities of by a data controller or data processor which is not *established* in the EEA to the extent the processing activity relates to:

a) offering of goods and services to data subjects in Norway, irrespective of whether a payment of the data subject is required; or

(b) the monitoring of their behavior, to the extent that such behavior takes place within Norway.

The DPA applies to processing of personal data by controller who is not established in Norway, but in a place governed by Norwegian law according to public international law.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Norwegian Data Protection Authority is:

Datatilsynet

www.datatilsynet.no

Together with other EEA countries (Iceland and Lichtenstein) the Norwegian Data Protection Authority became members of the EDBP however without voting rights and without the right to be elected as chair and vice-chair, for GDPR-related matters.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The government may issue further regulations as regards the duty to appoint a DPO. No such regulations have been issued yet.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;

- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;

- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Scope

The PDA and GDPR does not apply processing activities by physical persons for purely private or family purposes or for processing activities within the justice administration sector. For processing activities for journalistic purposes or academic, artistic or literary expressions, only the following articles of GDPR will apply: 24, 26, 28, 29, 32 40 - 43 as well as some of the chapters on the PDA.

Age limit to consent to information society services

According to the PDA, the age limit to consent to information society services is 13 years.

Processing of special categories of personal data

Processing of special categories of personal data is allowed when necessary to perform rights or obligations within the field of employment law.

The Norwegian Data Inspectorate may authorize the processing of sensitive personal data where the processing is in the public interest.

The Norwegian Data Inspectorate can also issue specific regulations allowing for the processing of special categories of data.

Processing of information relating to criminal offences:

According to the PDA, the processing of information about criminal offences is subject to the regulations as GDPR article 9(2)(a), (c) and (f) as well as the PDA §§ 6,7 and 9, i.e. the same provisions as the processing of special categories of personal data.

Use of personal ID numbers

Personal ID numbers unique identifiers may only be processed where there are reasonable grounds to require proper identification and the use of personal ID numbers is necessary for such identification.

Specific rules on consent

The PDA contains provisions relating to processing of special categories of personal data for *eg*, scientific purposes) without the consent of the data subject:

- provided that the processing is covered by necessary warranties in accordance with the GDPR Article 89, paragraph 1, there is no specific general regulation as regards safeguards according to GDPR Article 89, paragraph 1.

Before processing special categories of data, the data controller should consult and seek advice from the Data Protection Officer (DPO) in accordance with GDPR Article 37.

The above-mentioned advice from the DPO must consider whether the processing will meet the requirements of GDPR and other provisions laid down in the Norwegian Implementation Act. The consultation obligation with the DPO does not apply if an assessment has been made of privacy implications according to GDPR Article 35.

The duty to consult with a DPO also applies to the extent that processing of special categories of data for statistics of scientific purposes is based on consent.

Exemption to data subject rights to access and information

The PDA contains some exemption to right to access and information according to GDPR Article 13-15 to if the information:

a) is of relevance for Norwegian foreign policy or national security

b) must be kept secret in order to prevent, investigate, disclose and prosecute criminal acts;

c) that is considered that inadvisable that the data subject obtains due to the health situation of the relevant person or the relationship to close relationships of such persons;

d) subject to duty of confidentiality by law

e) which only is found in text prepared for internal purposes and not disclosed to others

f) where disclosure would be in breach of obvious and fundamental private or public interests.

Any denial of access according to the above shall be provided by way of a written explanation.

The right of access according to GDPR Article 15 does not apply to the processing of personal data for archival purposes in the public interest, purpose related to scientific or historical research or statistical purposes in accordance with GDPR Article 89. No. 1 so far as:

a) it will require a disproportionate effort to give access or

b) the right of access will make it impossible or seriously impair the achievement of the specific purposes.

The right to rectification and restriction in accordance with GDPR Article 16 and 18 does not apply to processing for archival purposes in the public domain interest, purposes related to scientific or historical research or statistical purposes in accordance with GDPR Article 89 No. 1 as far as it is likely that the rights make it impossible or seriously impair the achievement of the specific purposes.

The above exemptions do not apply if the processing has legal effects or directly has factual effects for the data subject.

Access to employee email

A separate regulation issued under the Working Environmental Act contains the conditions and procedures that have to be followed for accessing employee emails by an employer. Access to employee email can only take place if there is a legitimate interest or if it is necessary to secure daily operations or if there is a suspicion that the email has been used in

such a manner that it is a clear violation of the working relationship or could lead to dismissal or termination of employment.

The employee shall, as far as possible, be given notice and be able to participate when access to email is made.

CCTV surveillance in the workplace

A separate regulation has also been adopted and contains obligations as to, for example, notifying that CCTV recording takes place as well as specific deletion obligations. It also applies to dummy cameras.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU - US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account

of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Fines

Fines my be imposed on public authorities. Furthermore the PDA sets out that fines under GDPR will also apply to a breach of GDPR article 10 (processing of data relating to criminal convictions) and 24 (obligation on the controller to implement appropriate technical and organizational measurements to demonstrate that processing is in accordance with GDPR).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address

which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (*eg,* an email address is likely to be 'personal data' for the purposes of the Act).

Pursuant to the Marketing Control Act (Nw: *Markedsføringsloven*) section 15, it is prohibited in the course of trade, without the prior consent of the recipient, to send marketing communications to natural persons using electronic methods of communication which permit individual communication, such as electronic mail, telefax or automated calling systems (calling machines).

Prior consent is however not required for electronic mail marketing where there is an existing customer relationship and the contracting trader has obtained the electronic address of the customer in connection with a sale. The marketing may only relate to the trader's own goods, services or other products corresponding to those on which the customer relationship is based.

At the time that the electronic address is obtained, and at the time of any subsequent marketing communication, the customer shall be given a simple and free opportunity to opt out of receiving such communications.

'Electronic mail' in the context of the Marketing Control Act means any communication in the form of text, speech, sound or image that is sent via an electronic communications network, and that can be stored on the network or in the terminal equipment of the recipient until the recipient retrieves it. This includes text and multimedia messages sent to mobile telephones.

Direct marketing emails must not conceal or disguise the identity of the sender. If the email is unsolicited, it shall clearly state that the email contains a marketing message upon receipt of the message (The Norwegian E-Commerce Act, Nw: *Ehandelsloven*, section 9).

ONLINE PRIVACY

Traffic Data

Traffic data is defined in Norwegian Regulation relating to Electronic Communications Networks and Electronic Communications Services (Nw: *Ekomforskriften* F16.02.2004 nr 401) section 7-1 as data which is necessary to transfer communication in an electronic communications network or for billing of such transfer services.

Processing of traffic data held by a Communications Services Provider ('CSP') (Nw: *Tilbyder*) may only be performed by individuals tasked with invoicing, traffic management, customer enquiries, marketing of electronic communications networks or the prevention or detection of fraud.

Traffic Data held by a CSP must be erased or anonymized when it is no longer necessary for the purpose of the transmission of a communication (Electronic Communications Act section 2-7 (Nw: *Ekomloven*). However, Traffic Data can be retained if it is being used to provide a value added service and consent has been given for the retention of the Traffic Data.

Location Data

Location data may only be processed subject to explicit consent for the provision of a value added service which is not a public

telephony service, and the users must be given understandable information on which data is processed and how the data is used. The user shall have the opportunity to withdraw their consent. See Norwegian Regulation relating to Electronic Communications Networks and Electronic Communications Services section 7-2.

Cookie Compliance

The Electronic Communications Act has been changed in accordance with directive 2009/136/EC regarding the use of cookies. According to section 2-7 b, the user must give their consent before cookies or any other form of data is stored in their browser. The users must receive clear and comprehensive information about the use of cookies and the purpose of the storage or access. However, obtaining user consent is not required if the cookie solely has the purpose of transferring communication in an electronic network, or if it is deemed to be necessary for the delivery of a service requested by the user. The user's consent to processing may be expressed by using the appropriate settings of a browser or other application. Where the use of a cookie involves processing of personal data, the service providers will have to comply with the additional requirements of the Data Protection Act.

KEY CONTACTS

Petter Bjerke
Partner
T +47 2413 1654
petter.bjerke@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

PAKISTAN

Last modified 15 February 2019

LAW

Pakistan has not enacted data protection legislation.

DEFINITIONS

Definition of personal data

Not defined.

Definition of sensitive personal data

Not defined.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in Pakistan.

REGISTRATION

There is no registration requirement.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

There are no restrictions on the collection and processing of personal data.

TRANSFER

Pakistan does not specifically regulate data transfers, however, limitations apply.

Pakistan prohibits data transfers to any country that it does not recognize, including: Israel, Taiwan, Somaliland, Nagorno Karabakh, Transnistria, Abkhazia, Northern Cyprus, Sahrawi Arab Democratic Republic, South Ossetia and Armenia. This list may change from time to time. Additionally, data transfers to India must be justifiable by the transferor.

Data collated by banks, insurance firms, hospitals, defense establishments and other 'sensitive' institutions may not be transferred to any individual or body without authorization from the relevant regulator on a confidential basis. Such data is further regulated by contractual terms. In certain cases, data may not be transferred without authorization from the data subject.

However, banks and financial institutions must maintain confidentiality in banking transactions.

SECURITY

There are no data security requirements.

BREACH NOTIFICATION

There is no requirement to report data breaches to any individual or regulatory body.

ENFORCEMENT

There is no enforcement mechanism. Appropriate relief may be sought through courts of law having jurisdiction in the matter.

ELECTRONIC MARKETING

There is no electronic marketing regulation in Pakistan. Note that an earlier law promulgated in this regard has since lapsed.

ONLINE PRIVACY

There is no specific law that regulates the manner in which individuals private data may be stored or transmitted online.

The Prevention of Electronic Crimes Act, 2016 criminalizes unauthorized: access to information systems or data, copying or transmission of data and use of identity information. The Act further criminalizes "offenses against the dignity of a natural person," including the transmission of information through an information system which "harms the reputation or privacy of a natural person."

KEY CONTACTS

LMA Ebrahim Hosain
www.lma-eh.com

Darakhshan Sheikh Vohra
Partner
LMA Ebrahim Hosain
T +9221 3583 5101 – 104
d.vohra@lma-eh.com

Ali Qaisar
Associate
LMA Ebrahim Hosain
T +9221 3583 5101-104
a.qaisar@lma-eh.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

PANAMA

Last modified 28 January 2019

LAW

Panama has taken significant legislative steps to regulate data protection this year. In fact, Bill No. 665 of August 20, 2018, which regulates the protection of personal data, was approved by the National Assembly on October 24, 2018 and is—at the time of this writing—awaiting the President's approval in order to become law ("Draft Data Protection Law").

Until the Draft Data Protection Law is sanctioned, the primary laws that regulate data protection in Panama are:

- The Constitution
- The Criminal Code
- Several sectoral laws that regulate the matter in their respective jurisdictions

Electronic commerce is regulated by:

- Law 51 of July 22, 2008, as amended by Law 82 of November 9, 2012 ("Law 51")
- Executive Decree No. 40 of May 19, 2009 ("Decree 40")
- Executive Decree No. 684 of October 18, 2013 ("Decree 684")

The main purpose of both Law 51 and Decree 40 is to regulate the creation, use and storage of electronic documents and signatures in Panama through a registration process, and the supervision of providers of data storage services. Law 51 and Decree 40 provide for enforcement through the General Directorate of Electronic Commerce (Direccion General de Comercio Electronico) (DGCE).

Additionally, under Panamanian criminal law, individuals or entities that unlawfully access personal data are criminally liable pursuant to articles 289 and 290 of the Panamanian Criminal Code.

DEFINITIONS

Definition of personal data

Personal Data is not expressly defined under Panamanian law.

Definition of sensitive personal data

'Sensitive Personal Data' is not defined under Panamanian Law.

NATIONAL DATA PROTECTION AUTHORITY

Currently there is no National Data Protection Authority.

For electronic commerce, the national authority is:

The General Directorate of Electronic Commerce
(*Dirección General de Comercio Electrónico*)

Plaza Edison, Sector El Paical, Floors 2 & 3.

T (507) 560-0600
(507) 560-0700
F (507) 261-1942

contactenos@mici.gob.pa

REGISTRATION

There is no registration required for the processing of Personal Data under the current legislation.

Under Decree 40, electronic data storage companies and companies engaged in online electronic signature verification must register with the DGCE. For companies otherwise engaged in electronic commercial activities, registration with the DGCE is voluntary and can be completed online, free of charge. Registration must occur no later than 15 days prior to the commencement of data processing activities and shall include, inter alia, the following information:

- Name of the company
- Company´s physical address, telephone and fax number
- Legal representative of the company
- Company´s Internet address or URL
- Contact email provided by company to customers
- Public Registry and Ministry of Commerce Registration Information
- In the event that an undertaken activity requires specific authorization or permits, evidence thereof
- Tax Identification Number
- Description of services offered by the company, including pricing information and applicable taxes
- The company's code of conduct

Law 51 and Decree 40 set forth certain additional registration requirements for companies that are engaged in each of the activities for which registration is mandatory.

Further, pursuant to recently-enacted regulations, individuals or entities who wish to electronically interact with government entities must first register by activating a user account and executing a release form that is available both physically and online. To the extent necessary, government entities may also request a petitioner´s consent to access such petitioner's personal information that is available on a different government entity's system.

DATA PROTECTION OFFICERS

Appointment of a data protection officer is not required under current law.

COLLECTION & PROCESSING

In Panama, personal information is protected at the constitutional level. The Constitution provides that every person has a right of access to his / her personal information contained in data banks or public or private registries and to request their correction and protection, as well as their deletion in accordance with the provisions of the law. It also states that such information may only be collected for specific purposes, subject to the consent of the person in question, or by order of a competent authority based on the provisions of the law. The disclosure of personal information without consent is also prohibited by the Panamanian Criminal Code. Criminal penalties apply to the disclosure of personal information where the disclosure causes harm to the affected individual. Law 51 specifically establishes that this criminal law prohibition applies to electronically stored information.

Panamanian law further requires that providers of online data storage services take reasonable measures to ensure that company personnel who have access to confidential information:

- Do not have a criminal record
- Have obtained the necessary technical skills to handle such data and information
- Possess reasonable knowledge of existing legal restrictions related to the disclosure of such information

Although the last requirement is specifically intended to apply to entities that provide online data storage services, it is possible that it could also be construed to apply to any company engaged in electronic commerce.

TRANSFER

With regards to personal data, the Constitution states that individuals must give their consent in order for their personal data to be transferred or processed in any way.

Additionally, although the Panamanian e-commerce regulatory framework is not yet fully developed, the existing regulations follow the constitutional principle that the consent of the affected data subject is required for the transfer of any personal information.

Pursuant to Law 51, when a customer provides his / her email address during the process of acquiring or subscribing to a service offered online, the company providing such service must disclose to the customer its intent to use the email address in the future for commercial communications and, further, must obtain the customer's express consent for such purposes.

The client or customer must also be able to withdraw such consent easily, through a simple process made available by the provider of the service.

While the manner in which this restriction appears to have been drafted suggests that it applies exclusively to online service providers, its broader application to all companies that sell products online or are engaged in e-commerce activities is possible.

SECURITY

There are no security requirements under the current law regarding the protection of personal data.

Decree 40 establishes certain security requirements—applicable only to electronic data storage and electronic signature verification companies—for which registration with the DGCE is mandatory. The main requirements are adherence to the security standards periodically published by the DGCE, and the performance of annual self-audits, the results of which must be filed with the DGCE in order for the company to renew its registration. In addition, these companies must create a disaster recovery plan that allows such providers to re-establish regular operations within 12 hours of the occurrence of a disruptive event.

No similar provisions have been enacted with respect to companies who engage in other types of e-commerce (*ie*, those for which registration is voluntary).

BREACH NOTIFICATION

There are no breach notifications under the current legislation for Personal Data Protection.

Law 51 does not require breach notification to the affected parties.

However, the Panamanian Procedural Criminal Code does require individuals that have third party goods or interests under their care to report crimes affecting such goods or interest to the authorities. Given that article 289 and 290 of the Criminal Code make the theft of information a criminal offense, the preceding general provision may require the reporting of such crime to the authorities.

ENFORCEMENT

The DGCE is responsible for enforcement of the existing e-commerce and related regulations, including the publication of additional complementary regulations. Sanctions include the suspension or permanent ban of the activities of companies that infringe certain regulations, as well as fines of up to US$150,000.

ELECTRONIC MARKETING

With respect to email advertising, Panamanian law requires that all such emails:

- State that they are commercial communications
- Include the name of the sender
- Set forth the mechanism through which the recipient may choose not to receive any further communications from the particular sender

These requirements apply to other promotional offers as well.

Further, although opt-out tools are not prohibited, the client's initial opt-in consent is specifically required if an entity wishes to use the client's email for advertising purposes. Further, although no specific prohibition has been enacted with respect to the use of information for online advertising, obtaining the customer's consent is always preferable.

ONLINE PRIVACY

The existing regulatory framework does not yet address location data, cookies, local storage objects or other similar data-gathering tools.

KEY CONTACTS

Galindo, Arias & Lopez
gala.com.pa/

Diego Herrera
T +507 303 0303
dherrera@gala.com.pa

James Sattin
T +507 303 0303
jsattin@gala.com.pa

Jose Luis Sosa
T +507 303 0303
jsosa@gala.com.pa

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

PERU

Last modified 28 January 2019

LAW

Article 2 of the Political Constitution of Peru sets forth certain fundamental rights that every person has, including a right to privacy regarding information that affects personal and family privacy, which was the basis for the creation of a law that specifically protects the use of personal data of any natural person and applies to both private and state entities.

The Personal Data Protection Law N° 29733 (PDPL) was enacted in June 2011. In March 2013, the Supreme Decree N° 003-2013-JUS-Regulation of the PDLP (Regulation) was published in order to develop, clarify and expand on the requirements of the PDPL and set forth specific rules, terms and provisions regarding data protection.

Together, the PDLP and its Regulation are the primary data protection laws in Peru.

Further, the law regulating private risk centers and the protection of the owner of the information is Law N° 27489, enacted in 2001 and later amended several times. This law establishes the applicable provisions for activities related to risk centers and companies that handle:

- Information posing higher risks to individuals (*eg*, related to financial, commercial, tax, employment or insurance obligations or background of a natural or legal person that allows evaluating its economic solvency), and
- Sensitive personal data (according to the PDPL)

DEFINITIONS

Definition of personal data

Personal data is defined as information — regardless of whether numerical, alphabetic, graphic, photographic, acoustic — about personal habits or any other kind of information about an individual that identifies or may identify such individual by any reasonable means.

Definition of sensitive personal data

Sensitive personal data includes all of the following:

- Personal data created through biometric data which by itself renders a data subject identifiable
- Personal data regarding an individual's physical or emotional characteristics, facts or circumstances of their emotional or family life, as well as personal habits that correspond to the most intimate sphere
- Data referring to racial and ethnic origin
- Economic income, opinions or political, religious, philosophical or moral convictions
- Union membership
- Information related to physical or mental health, to sexual life or other similar information that affect the data subject's privacy

NATIONAL DATA PROTECTION AUTHORITY

The Directorate for the Protection of personal data, which is part of the General Directorate of Transparency, Access to Public Information and Protection of Personal Data (NDPA), is the primary agency in charge of enforcing data protection matters.

The NDPA's current address is:

Scipion Llona 350
Miraflores, L-18
Lima
Peru

Website

REGISTRATION

The National Registry for the Protection of Personal Data (NRPDP) maintains information about personal databases of public or private ownership and publishes a list of such databases to facilitate individuals' exercise of their rights of access to information, rectification, cancellation, opposition and others regulated in the PDPL and its Regulation.

In addition, the NRPDP maintains records of:

- Communications of cross-border flow of personal data
- The codes of conduct of the holders of personal databases, and
- The sanctions, precautionary or corrective measures imposed by the NDPA

The holders of personal databases must register in the NRPDP providing the following information:

- The name and location of the personal database
- The purposes and the intended uses of the database
- The identification of the owner of the personal database
- The categories and types of personal data to be processed
- Collection procedures and a description of the system for processing personal data
- The technical description of the security measures
- The recipients of personal data transfers

The cross-border transfer of personal data must be notified to the NDPA, including the information required for the transfer of data and registration of the database.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

The collection and processing of personal data requires the data subject's prior, informed, express and unequivocal consent. The consent may be expressed through electronic means.

The collection and processing of sensitive personal data requires the data subject's prior, informed, express and unequivocal consent, and must be expressed in writing.

The data subject's consent is not necessary if any of the following are true:

- The data are compiled or transferred for the fulfillment of governmental agency duties
- The data are contained or destined to be contained in a publicly available source

- The data are related to credit standing and financial solvency, as governed by applicable law (Law N° 27489)
- A law is enacted to promote competition in regulated markets, under the powers afforded by the Framework Law for Regulatory Bodies of Private Investmenton Public Services (Law N° 27332), provided that the information supplied does not breach the user's privacy
- The data are necessary for a contractual, scientific or professional relationship with the data subject, provided that such data is necessary for the development and compliance with such relationship
- The data are needed to protect the health of the data subject, and data processing is necessary, in circumstances of risk, for prevention, diagnosis, and medical or surgical treatment, provided that the processing is carried out in health facilities or by professionals in health sciences observing professional secrecy
- The data are needed for public interest reasons declared by law or public health reasons (both must be declared as such by the Ministry of Health) or to conduct epidemiological studies or the like, as long as dissociation procedures are applied
- The data are dissociated or anonymized
- The data are used by a nonprofit organization with a political, religious, ortrade union purpose, and refer to the data of its members within the scope of the organization´s activities
- The data are necessary to safeguard the legitimate interest of the data subject orthe data handler
- The data are being processed for purposes linked to money laundering and terrorist financing or others that respond to a legal mandate
- In the case of economic groups made up of companies that are considered subjects obliged to inform, the data is processed in accordance with the rules that regulate the Financial Intelligence Unit, so that they may share information with each other about their respective clients to prevent money laundering and financing of terrorism (as well as in other instances of regulatory compliance, establishing adequate safeguards on the confidentiality and use of the information exchanged)
- When the treatment is carried out in a constitutionally valid exercise of the fundamental right to freedom of information
- Others expressly established by law

If the data controller outsources the processing of the personal data to a third party (*ie,* a processor), such party must also comply with the relevant requirements of the PDLP (*eg*, to maintain personal data as confidential and to use the personal data only for the purposes authorized and modify inaccurate information).

Upon termination or expiration of the outsourcing agreement, the personal data processed must be deleted, unless the data subject provides express consent to do otherwise.

The processing of personal data by cloud services, applications and infrastructure is permitted, provided compliance with the provisions of the PDPL and its Regulation is guaranteed.

TRANSFER

Where personal data is transferred to another entity, recipients must be required to handle such personal data in accordance with the provisions of the PDPL and its Regulation.

Generally, data subject consent is required.

Cross-border transfers

The transferring entity may not transfer personal data to a country that does not afford adequate protection levels (protections that are equivalent to those afforded by the PDPL or similar international standards). If the receiving country does not meet these standards, the sender must ensure that the receiver in the foreign country is contractually obligated to provide 'adequate protection levels' to the personal data, such as via a written agreement that requires that the personal data will be protected in accordance with the requirements of the PDPL, or under one of the following circumstances:

- In accordance with international treaties in which Peru is a party
- For purposes of international judicial cooperation or international cooperation among intelligence agencies to combat
    - Terrorism
    - Drug trafficking

    - Money laundry
    - Corruption
    - Human trafficking, and
    - Other forms of organized crime
- When necessary for a contractual relationship with the data subject, or for a scientific or professional relationship
- Bank or stock transfers concerning transactions in accordance with the applicable law
- The transfer is performed to protect, prevent, diagnose or medically or surgically treat the data subject, or to perform studies of epidemiology or the like, provided a data dissociation procedure has been applied
- The owner of the personal data has given its prior, informed, express and unequivocal consent to the transfer to the inadequate jurisdiction
- Other exempt purposes established by the Regulations

For both domestic and cross-border transfers, the recipient must assume the same obligations as the transferor of the personal data. The transfer must be formalized, such as by binding written contract, and capable of demonstrating that the holder of the database or the data controller communicated to the recipients the conditions in which the data subject consented to their processing.

SECURITY

Database holders and data handlers must adopt technical, organizational and legal measures necessary to guarantee the security of the personal data they hold. The measures taken must ensure a level of security appropriate to the nature and purpose of the personal data involved.

The Agency has passed a Directorial Resolution N° 019-2013-JUS/DGPDP (hereafter, the 'Security Directive'). This Security Directive establishes different standards depending on the features of the database, including:

- Number of data subjects whose data are contained in the database
- Number of fields of the database (eg, name, address, phone number)
- Existence of sensitive data
- Owner of the database (an individual or entity)

The following security measures must be taken with respect to the loss of a personal data bank:

- Backup copies of personal data must be made to allow recovery in case of loss or destruction
- Any recovery of personal data, from the backup, must have the authorization of the person in charge of the personal data bank
- Proof of recovery of personal data must be performed to verify that backup copies can be used if they are required

For digital information, it is important to mention that the computer systems that handle databases or process personal data must include in their operation records that keep all types of interaction with logical data, so as to identify the users, changes, consultations, starting and closing hours of a session and other actions that are carried out. These records will allow the access of competent, authorized and identified personnel only.

Further, it is necessary to establish the following:

- Security measures related to the authorized accesses to the data by procedures of identification and authentication that guarantee the confidentiality and integrity of the data
- Necessary mechanisms for correct application of the procedures for making backup copies and recovery of the data in order to guarantee the reconstruction in the status they had at the time of the loss or destruction

The applicable measures in which the information must be processed, stored or transmitted—taking into account the controls, policies, standards and recommendations related to physical and environmental security—are established in the following documents:

- Peruvian Technical Standards 'NTP- ISO/IEC 17799: 2007 EDI. Technology of Information. Code of Good Practice for the

management of the security of the information. 2nd Edition'
- 'NTP ISO/IEC 27001: 2008 EDI Technology of Information. Security Techniques. Systems of Management of Information Security. Requisites.'

BREACH NOTIFICATION

The holder of a database (and processor, where applicable) is required to implement security measures to prevent the unauthorized access to personal data.

As a consequence, an implied obligation would be to adopt all corrective measures in the event of a data breach to minimize the damages it may cause to the data subjects. For that reasons, the Security Directive establishes security measures against:

- The loss of the personal database, and
- An unauthorized processing of the personal database

In this way, any case of data breach should be communicated to the data subjects as soon as it is confirmed. The database owner must inform the data subject of 'any incident that significantly affects their property or their moral rights', as soon as the occurrence of the incident is confirmed.

The minimum information to be provided in a notice includes a description of:

- The incident
- Personal data disclosed
- Recommendations to the data subject
- Corrective measures implemented

Mandatory breach notification

No breach notification to the NDPA is required.

ENFORCEMENT

The General Directorate of Sanctions (part of the NDPA) instructs on and resolves, in the first instance, violations and imposes sanctions as well as conducts and develops the research phase according to Article 115 of the Regulation of the PDLP.

The General Directorate for the Protection of personal data (also part of the NDPA) resolves in the second and last instance the sanctioning procedure and its decision exhausts the administrative route.

Possible sanctions for breaching data protection standards vary depending on the nature or magnitude of the offense:

- The fine applicable to minor infringement ranges from S/.650 to S/.6,200
- The fine applicable to severe infringements ranges from S/.6,200 to S/.62,000
- The fine applicable to very severe infringements ranges from S/.62,000 to S/.124,000

The NDPA is also authorized to impose additional fines up to S/.12,500, if the offender, despite being found liable and sanctioned as a consequence thereof, fails to remedy the unlawful practice. These are applicable in addition to civil and criminal liability.

ELECTRONIC MARKETING

The PDPL does not expressly regulate electronic marketing. However, the PDPL does apply to electronic marketing activities if personal data is processed as a result.

If consent is obtained through electronic media, the notice requirements can be met by publishing accessible and identifiable privacy policies with the relevant consent language and mechanism. The PDPL establishes the possibility of obtaining express consent by presenting the option to agree with the privacy policies in clickable ways (*eg*, by clicking, ticking a box).

Written consent may be provided by other options, including:

- Through an electronic signature
- A written document possible to read or print
- A mechanism or procedure that allows one to identify the subject and to receive his consent through a written text
- A pre-established text as long as it is easily visible, legible and written in simple language

The laws governing electronic signatures are:

- Law N° 27291
- The Digital Certificates and Signatures Law (Law N° 27269)
- Supreme Decree N° 052-2008-PCM

Note that expressing the will in any of the regulated forms does not eliminate the other requirements of consent referring to that consent must be informed, and freely given.

Separately, specific regulation for electronic marketing can be found in the Anti-Spam Law, N° 28493 and its regulations (Supreme Decree N° 031-2005-MTC). These apply to unsolicited commercial emails defined as electronic mail messages that originate in Peru and contain promotional commercial information regarding goods and services, events, competitions and / or activities that are traded, offered, sponsored or organized by company individuals.

Unsolicited commercial emails must contain:

- The word PUBLICIDAD (which means advertisement) at the beginning of the subject field in the email
- Name or corporate name, complete domicile and email address of the sender (including the complete name of a contact person)
- The inclusion of an email address to which the receiver can send an email in order to opt out of receiving more unsolicited commercial emails, or another Internet-based mechanism that enables opt-out

Emails will not be considered unsolicited in the following cases:

- If the recipient has previously requested (expressly and in writing) to receive such notifications
- If there is a prior contractual relationship and the commercial communications sent refer to goods and services of the contracting company that are similar to goods or services contracted for

According to the Consumer Protection Code Law N° 29571, the following commercial activities require prior, informed, express and unequivocal consent to promote products and services:

- Use of call centers
- Use of telephone call systems
- Bulk text messages or emails
- Telemarketing services

ONLINE PRIVACY

The PDPL does not expressly regulate online privacy, including cookies and location data. However, the PDPL will apply if personal data is collected and processed using these mechanisms.

This requires that the use and deployment of cookies, location data or another personal data that will be collected must comply with data privacy laws. The data subject's consent must be obtained before cookies and/or location data can be used.

With respect to criminal law enforcement, Legislative Decree N° 1182 permits the National Police of Peru to access the location and geolocation of mobile phones or electronic devices of similar nature in cases of *flagrante delicto*.

It establishes the obligation for public communications services providers and public entities to keep the data from their users derived from telecommunication services during the first 12 months in computer systems an additional period of 24 months in an electronic storage system. Such service providers are bound to provide the location and geolocation data immediately, 24 hours a

day, 365 days of the year, under warning of being liable to the responsibilities regarded by law in the event of noncompliance.

KEY CONTACTS

Ricardo Escobar
Partner
DLA Piper Pizarro Botto Escobar
T +1 511 616 1200
rescobar@dlapiperpbe.com

Daniel Flores
Associate
DLA Piper Pizarro Botto Escobar
T +1 511 616 1200
dflores@dlapiperpbe.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

PHILIPPINES

Last modified 25 January 2017

LAW

The Philippines recently enacted the Data Privacy Act of 2012 (the 'Act') or Republic Act No. 10173, which took effect on 8 September 2012.

DEFINITIONS

Definition of personal data

Personal Information is defined in the Act as 'any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.'

The Act, in addition to defining 'Personal Information' that is covered by the law, also expressly excludes certain information from its coverage. These are:

- information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:
    - the fact that the individual is or was an officer or employee of the government institution
    - the title, business address and office telephone number of the individual
    - the classification, salary range and responsibilities of the position held by the individual, and
    - the name of the individual on a document prepared by the individual in the course of employment with the government.
- information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services
- information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit
- personal information processed for journalistic, artistic, literary or research purposes
- information necessary in order to carry out the functions of a public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of

their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act ('CISA').

- information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Philipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws, and

- personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

Definition of sensitive personal data

Sensitive Personal Information is defined in the Act as personal information:

- about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations

- about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offence committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings

- issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or cm-rent health records, licences or its denials, suspension or revocation, and tax returns, and

- specifically established by an executive order or an act of Congress to be kept classified.

NATIONAL DATA PROTECTION AUTHORITY

The Act provides for the creation of a National Privacy Commission. As of 21 January 2015, the National Privacy Commission has not been constituted.

REGISTRATION

There is no system of mandatory registration provided in the Act.

DATA PROTECTION OFFICERS

The Personal Information Controller of an organisation must appoint a person or persons who shall be accountable for the organisation's compliance with the Act, and the identity of such person or persons must be disclosed to the data subjects upon the latter's request. The Act does not specifically provide for the citizenship and residency of the data protection officer. The Act likewise does not specifically provide for penalties relating to the incorrect appointment of data protection officers.

COLLECTION & PROCESSING

The collection and processing of Personal Information must comply with the general principle that Personal Information must be:

- collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only

- processed fairly and lawfully

- accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted

- adequate and not excessive in relation to the purposes for which they are collected and processed
- retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defence of legal claims, or for legitimate business purposes, or as provided by law, and
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed:
    - provided that personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods, and
    - provided, further, that adequate safeguards are guaranteed by said laws authorising their processing.

In addition, the processing of personal information must meet the following criteria, otherwise, such processing becomes prohibited:

- the data subject has given his or her consent
- the processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract
- the processing is necessary for compliance with a legal obligation to which the personal information controller is subject
- the processing is necessary to protect vitally important interests of the data subject, including life and health
- the processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate, or
- the processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

The processing of sensitive personal information is prohibited, except in the following cases:

- the data subject has given his or her specific consent prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing
- the processing is provided for by existing laws and regulations, provided that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information, and the consent of the data subjects is not required by law or regulation permitting the processing of the sensitive personal information or the privileged information
- the processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing
- the processing is necessary to achieve the lawful and non-commercial objectives of public organisations and their associations, provided:
    - such processing is only confined and related to the bona fide members of these organisations or their associations
    - the sensitive personal data are not transferred to third parties, and
    - the consent of the data subject was obtained prior to processing

- the processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured, or

- the processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

TRANSFER

The transfer of Personal Information is permitted without any restrictions or prerequisites, but the Personal Information Controller remains responsible for personal information under its control or custody that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. The transfer, however, of sensitive personal information to third parties is prohibited.

SECURITY

The personal information controller must implement reasonable and appropriate organisational, physical and technical measures to protect personal information against any type of accidental or unlawful destruction, such as from accidental loss, unlawful access, fraudulent misuse, unlawful destruction, alteration, contamination and disclosure, as well as against any other unlawful processing.

The determination of the appropriate level of security must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organisation and complexity of its operations, current data privacy best practices and the cost of security implementation.

In addition, the security measures to be implemented must include the following, which are subject to guidelines that the National Privacy Commission may issue:

- safeguards to protect its computer network against accidental, unlawful or unauthorised usage or interference with or hindering of their functioning or availability

- a security policy with respect to the processing of personal information

- a process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach, and

- regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

The personal information controller is obligated to ensure that third parties processing personal information on its behalf shall implement the security measures required by the Act.

The obligation to maintain strict confidentiality of personal information that are not intended for public disclosure extends to the employees, agents or representatives of a personal information controller who are involved in the processing of such personal information.

BREACH NOTIFICATION

The Personal Information Controller is required to promptly notify the National Privacy Commission and the affected data subjects when it has reasonable belief that sensitive personal information or other information has been acquired by an unauthorised person, and that:

- such personal information may, under the circumstances, be used to enable identity fraud, and

- the Personal Information Controller or the National Privacy Commission believes that such unauthorised acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach.

Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. The National Privacy Commission may also authorise postponement of notification where such notification may hinder the progress of a criminal investigation related to a serious breach.

Notification is not required if the National Privacy Commission determines:

- that notification is unwarranted after taking into account compliance by the Personal Information Controller with the Act and the existence of good faith in the acquisition of personal information, or
- in the reasonable judgment of the National Privacy Commission, such notification would not be in the public interest or in the interests of the affected data subjects.

ENFORCEMENT

The National Privacy Commission is responsible for ensuring compliance of the Personal Information Controller with the Act. It has the power to receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicise any such report. Additionally, the National Privacy Commission can issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest.

The National Privacy Commission, however, cannot prosecute violators for breach of the Act for which criminal penalties can be imposed. The Department of Justice is tasked with the prosecution for violations of the Act that are punishable with criminal sanctions.

The following actions are punishable by the Act with imprisonment in varying duration plus a monetary penalty:

- processing of personal information or sensitive personal information:
    - without the consent of the data subject or without being authorised by the Act or any existing law, or
    - for purposes not authorised by the data subject or otherwise authorised under the Act or under existing laws
- providing access to personal information or sensitive personal information due to negligence and without being authorised under this Act or any existing law
- knowingly or negligently disposing, discarding or abandoning the personal information or sensitive personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection
- knowingly and unlawfully, or violating data confidentiality and security data systems, breaking in any way into any system where personal and sensitive personal information is stored
- concealing the fact of such security breach, whether intentionally or by omission, after having knowledge of a security breach and of the obligation to notify the National Privacy Commission pursuant to Section 20(f) of the Act
- disclosing by any personal information controller or personal information processor or any of its officials, employees or agents, to a third party personal information or sensitive personal information without the consent of the data subject and without malice or bad faith, and

- disclosing, with malice or in bad faith, by any personal information controller or personal information processor or any of its officials, employees or agents of unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her.

ELECTRONIC MARKETING

In 2008, the Department of Trade and Industry, the Department of Health, and the Department of Agriculture issued a joint administrative order implementing the Consumer Act of the Philippines (Republic Act No. 7394) and the E-Commerce Act (Republic Act No. 8792). The Joint DTI-DOH-DA Administrative Order No. 01 (the 'Administrative Order') provides rules and regulations protecting consumers during online transactions, particularly on the purchase of products and services. It covers both local and foreign-based retailers and sellers engaged in e-commerce.

The Administrative Order particularly requires retailers, sellers, distributors, suppliers or manufacturers engaged in electronic commerce with consumers to refrain from engaging in any false, deceptive and misleading advertisement prohibited under the provisions of the Consumer Act of the Philippines.

In line with the Administrative Order's provision on fair marketing and advertising practices, retailers, sellers, distributors, suppliers or manufacturers engaged in electronic commerce are mandated to provide:

- fair, accurate, clear and easily accessible information describing the products or services offered for sale such as the nature, quality and quantity thereof
- fair, accurate, clear and easily accessible information sufficient to enable consumers to make an informed decision whether or not to enter into the transaction, and
- such information that allows consumers to maintain an adequate record of the information about the products and services offered for sale

Section 4(c)(3) of the CPA was struck down by the Supreme Court for violating the constitutionally guaranteed freedom of expression.

ONLINE PRIVACY

The CPA is the first law in the Philippines which specifically criminalises computer crimes. The law aims to address legal issues concerning online interactions. The CPA does not define nor does it particularly refer to online privacy, however, it penalises acts that violate an individual's rights to online privacy, particularly those interferences against the confidentiality, integrity and availability of computer data and systems.

All data to be collected or seized or disclosed will require a court warrant. The court warrant shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce showing that there are:

- reasonable grounds to believe that any of the crimes penalised by the CPA has been committed, or is being committed, or is about to be committed
- reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes, and
- no other means readily available for obtaining such evidence.

The integrity of traffic data shall be preserved for a minimum period of six months from the date of the transaction.

Courts may issue a warrant for the disclosure of traffic data if such disclosure is necessary and relevant for the purposes of investigation in relation to a valid complaint officially docketed.

No law in this jurisdiction currently deals with the subject of Location Data or the regulation of the use of Cookies.

KEY CONTACTS

Romulo Mabanta Buenaventura Sayoc & De Los Angeles
www.romulo.com/

Eileen Rosario Cordero-Batac
Partner
T +63 2 555 9555
eileen.batac@romulo.com

Catherine O. King Kay
Associate
T +63 2 555 9555
catherine.kingkay@romulo.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

POLAND

Last modified 11 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

As a member of the European Union, Poland implemented the EU Data Protection Directive 95/46/ EC in the Personal Data Protection Act of August 29, 1997 (consolidated text: Journal of Laws of 2016, item 922, hereinafter referred to as the previous PDPA). A number of provisions of the Telecommunications Act of 16 July 2004 (consolidated text: Journal of Laws 2017, item 1907, hereinafter referred to as the Telecommunications Act) are applicable to the processing of personal data by providers of publicly available telecommunications services and a number of sector specific statutes relating to, among others, employment and banking matters also contain specific regulations on the processing of personal data.

In relation to the GDPR, on September 12, 2017, two draft acts on personal data protection law were published in Poland. The first one was the draft of the PDPA which came into force on May 25, 2018 (Personal Data Protection Act of 10 May 2018 (Journal of Laws of 2018, item 1000, hereinafter referred to as the new PDPA), while the second is the draft act on the provisions implementing the new PDPA (it contains a number of amendments of sectorial regulations (hereinafter referred to as the draft of the second act). The entry into force of the draft of the second act has been delayed and, according to the latest information, the legislative procedure may not be completed before March 2019.

The two new pieces of legislation are aimed at implementing the GDPR into the Polish legal order, as well as regulating the matters in which the GDPR leaves a certain regulatory freedom for EU Member States. The new PDPA establishes a

new supervisory body – the President of the Office for Personal Data Protection (hereinafter referred to as the President of the Office), which has a much wider range of powers than the previous DPA (Inspector General for the Protection of Personal Data – hereinafter referred to as the Inspector General).

The amendments to the sectorial regulations included in the draft of the second act will affect, among others, employment, banking and insurance regulations. The act is still going through the legislative procedure (the most recent draft was published on November 23, 2018) and it is subject to proceedings in Parliament. According to the latest information, the act will be applicable from late Spring 2019.

DEFINITIONS

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The PDPA does not include any local derogations to the definitions set out in GDPR. The most recent draft of the second act also does not include any local derogations, however, it is still going through the legislative procedure and may be subject to change.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects

only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The President of the Office for Personal Data Protection.

Office of the President for Personal Data Protection
Urzad Ochrony Danych Osobowych
Stawki 2
00-193 Warsaw, Poland

Tel. +48 22 531 03 00
Fax +48 22 531 03 01
kancelaria@uodo.gov.pl

Helpline (in Polish only): tel. +48 606-950-000 is open from Monday to Friday from 10 am to 1 pm.

The Office of the President is open from Monday to Friday from 8 am to 4 pm.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Under the previous PDPA (in force until May 25, 2018), as a general rule, data controllers that process personal data were obligated to notify the Inspector General about the data filing system containing that data. The Inspector General kept a register of data controllers and data filing systems, which was available to the public.

This obligation does not longer exists under the new PDPA.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities

(Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection laws and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

According to the new PDPA, the appointment of a Data Protection Officer (DPO) must be notified to the supervisory authority within 14 days. The notification should include the name and email address of the DPO or his or her phone number. Any changes to the information provided or the dismissal of a DPO should also be notified within 14 days. The entity who appointed the DPO shall make available the DPO's details on its website or in a generally accessible manner at a place of pursuit of activity (if it does not have its own wesbite). According to official guidance from the Polish DPA, the contact details of the DPO should be easily accessible, not hidden somewhere in long documents such as a privacy policy etc.

The draft of the second act includes the possibility to designate a person to replace the DPO during their absence (*eg,* temporary absence). However, it would be necessary to inform the Polish DPA about the designation. All rules and requirements for DPOs would also be applicable to this person.

Please note that the whole draft of the second act is still going through the legislative procedure and is likely to be further amended.

If a person was officially appointed as an Information Security Officer (ABI) under the previous PDPA, this person automatically became a DPO for the data controller until September 1, 2018, and provided that the appointment was notified to the President of the Office before that date, the person continues to serve as a DPO after that date.

If the data controller is obliged to appoint a DPO in accordance with Article 37 of the GDPR but did not appoint one under the previous PDPA, the appointment of the DPO should have take place and been notified to the President of the Office before July 31, 2018.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous,*" and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices

- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to re-purpose personal data – *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that

further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision taking, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (*ie,* opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The new PDPA includes some derogations from the GDPR. However, the draft of the second act is likely to introduce more provisions which elaborate on the provisions of the GDPR on the collection and processing of personal data. It is important to note that the Polish legislator has decided to include derogations regarding labour law both in the new PDPA and in the draft of the second act.

The new PDPA contains provisions amending, among others, the Labour Code. These provisions provide for circumstances under which the employer can carry out video surveillance, email monitoring and other employee monitoring activities. Video surveillance may be implemented if it is necessary to ensure the safety of employees or the protection of property or production control or to keep information, the disclosure of which could cause damage to the employer, confidential. Monitoring of work emails may be implemented if it is necessary to ensure maximum work efficiency and the proper use of work tools made available to the employees. The scope, means and purposes of the employee monitoring must be provided to the employees via workplace regulations or other, exhaustively listed, means at least two weeks before the monitoring starts. The legality of a particular monitoring scheme should be assessed on a case-by-case basis.

The new PDPA also prescribes the maximum retention period of the information obtained from video monitoring (it must not be stored indefinitely). The mater can be retained for three months after the recording took place, unless the recording constitutes (or may constitute) evidence in legal proceedings. In this case, the material may be stored until the final decision in the proceedings is issued. In relation to the retention period of information obtained via any other form of employee monitoring, the general rules of the GDPR apply - the materical can be retained as long as is reasonably needed for the purposes for which it was collected. The remaining changes to the Labout Code are included in the draft of the second act.

For example, the employer may process the personal data of its employees or job applicants referred to in Article 9(1) with consent however only if the data was given on the data subject's own initiative. Another significant amendment is to the scope of data requested when applying for a job. Although address as well as parents' names are no longer needed, contact details should be provided. Changes in video surveillance would allow an employer to locate cameras in sanitary areas upon prior consent from the enterprise trade union or the employee representative who has been chosen in the way prescribed by an employer.

Please note that the whole draft of the second act is still going through the legislative procedure and is likely to be further amended.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor

and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
d. The transfer is necessary for important reasons of public interest
e. The transfer is necessary for the establishment, exercise or defense of legal claims
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
g. The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State. A transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

In the case of the transfer of personal data to a third country, the new PDPA does not impose any additional requirements concerning notifications to or registrations with the President of the Office.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident,
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

The new PDPA does not include any derogations from the GDPR.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

In Poland, data controllers from the telecommunications sector are required to inform sectoral regulators of any data security breach. Pursuant to the Telecommunications Act, the provider of telecommunications services is obliged to immediately (and no later than within 3 days of learning about a data breach) notify the President of the Office about any data breach. If a data breach could have a negative impact on the rights of a subscriber or end user (*ie,* a natural person), the service provider should immediately (and no later than within 3 days of learning about the data breach) also inform the subscriber or end user (in addition to informing the President of the Office) about the breach.

The breach notification obligations under the Telecommunications Act are replaced by the breach notification obligations under the terms specified in Commission Regulation (EU) No. 611/2013 of June 24, 2013 regarding measures applicable to notification of personal data breaches under Directive 2002/58/ EC of the European Parliament and of the Council on privacy and electronic communications (Regulation 611/2013). Please note that the amendments are included in the draft of the second act.

A personal data breach should be reported by the provider of telecommunications services to the President of the Office immediately, and no later than 24 hours after the detection of the personal data breach. This deadline results from Article 2 section (2) of the Regulation 611/2013. Because this period is shorter than the period indicated in the GDPR, telecommunications undertakings will have to make every effort to send the information required by law within 24, not 72, hours. Therefore, the personal data breach should be notified electronically by filling out the appropriate form.

If a data breach could have a negative impact on the rights of a subscriber or end user (*ie,* a natural person), the service provider should also - no later than within 3 days of learning about the data breach (according to the Telecommunication Act) - inform the subscriber or end user (in addition to informing the President of the Office) about the breach. The draft of the second act contains provisions that the service provider shall immediately (*ie,* without undue delay) inform the subscriber or end user referring to Regulation 611/2013.

Please note that the legislative procedure is still in progress and this matter should be reviewed again in due time.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define undertaking and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of undertaking. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called look through liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- Data subjects' rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The President of the Office is responsible for the enforcement of Polish data protection law and as such is entitled to carry out audits of data controllers in order to determine their compliance with the regulations on the protection of personal data and to impose administrative fines, by means of an administrative decision, pursuant to Article 83 of the GDPR.

The new PDPA provides for a lower level of fines that can be imposed on public authorities for breaching the GDPR – the maximum amount is PLN 100,000 (approx. EUR 25,000).

The new PDPA maintains the criminal liability for individuals who process personal data:

- A person who processes personal data where such processing is forbidden or where he or she is not authorized to carry out such processing may be liable to a fine, a partial restriction of freedom, or imprisonment of up to two years (or three years if special categories of personal data are processed).
- A person who prevents or hinders the performance of inspection activities conducted by the President of the Office (or its delegated inspectors) may be liable to a fine, a restriction of liberty, or imprisonment of up to two years.

As only individuals (and not legal entities) may be prosecuted for criminal offences, the person who may potentially face criminal charges would be a member of the management board (the person performing the role of data controller in a legal entity) or an employee authorized to process personal data (*eg*, a data protection officer or human resources officer).

Currently, there is limited information on the practice of enforcement under GDPR in Poland. According to latest information at the time of this update, the Polish supervisory authority has not imposed any fines yet.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Electronic marketing activities are subject to the regulation of Polish data protection law, i.e. the Act of July 18, 2002 on Providing Services by Electronic Means (consolidated text: Journal of Laws of 2017, item 1219, hereinafter referred to as

the PSEM) and the Telecommunications Act.

The processing of personal data for its own marketing purposes by a data controller (as well as other companies from the group) may be based on Article 6 sec. 1(f) of the GDPR – legitimate interests of the data controller, and it does not require separate consent. However, the data subject may always object to such processing. Nevertheless, if marketing activities relate to products and services of third parties, prior consent for such processing is necessary.

Apart from consent to the processing of personal data (if it is required), the PSEM imposes an obligation to obtain separate consent to the sending of commercial information by electronic means, (*eg,* by email and SMS) to a specified recipient (natural person). Therefore, a service provider is obliged to obtain the relevant consent before sending the commercial information (by email or SMS) to a natural person. On the other hand, it is permitted to send such information without prior consent to recipients that are legal persons to a general email addresses (such as office@company.com) and to a specific employee's business email address (such as name.surname@company.com). According to the current draft of the second act, the consent under the PSEM must comply with the GDPR requirements as regards the format. Sending commercial information without consent is considered to be an act of unfair competition and a service provider should be able to provide evidence that it has obtained consent.

Pursuant to the Telecommunications Act, using end telecommunications devices (for instance, to present a marketing offer during a telephone call) or automated calling systems for direct marketing requires the obtaining of another consent declaration from the recipient (subscriber or end user). In practice, the relationship between the abovementioned regulations (especially between the provisions of the new PDPA and the Telecommunications Act) and the scope of particular consent declarations that should be obtained by service providers is not perfectly clear in this regard. However, it seems that, generally, the consent to direct marketing by means of telecommunications devices and automated calling systems should be obtained separately from the consent to the processing of personal data (if required) and to consent to the sending of commercial information by electronic means. According to the current draft of the second act, the consent of the subscriber or the end user must comply with the GDPR requirements as regards the format. The legislative procedure is still in progress and the matter should be reviewed again in due time.

Enforcement and sanctions

Failing to meet the obligations to obtain consent to direct marketing by means of telecommunications devices and automated calling systems may be subject to a fine of up to 3% of the revenues of the fined company for the previous calendar year. The fine is imposed by the President of the Office of Electronic Communication (hereinafter referred to as the President of the OEC). In addition, the President of the OEC may impose a fine on a person holding a managerial position in the company (such as a member of the management board) of up to 300% of his or her monthly remuneration.

Sending marketing information by electronic means without the consent of the recipient may be subject to a fine of up to PLN 5,000 (approx. EUR 1,200) under the provisions of the PSEM and is considered to be an act of unfair competition (*ie,* a practice that infringes collective consumer interests) and thus may be subject to a fine of up to 10% of the revenues of the fined company for the previous calendar year (subject to separate regulations).

ONLINE PRIVACY

The Telecommunications Act regulates the collection of transmission and location data and the use of cookies (and similar technologies).

Transmission data

The processing of transmission data (understood as data processed for the purpose of transferring messages within telecommunications networks or charging payments for telecommunications services, including location data, which should be understood as any data processed in a telecommunications network or as a part of telecommunications services indicating the

geographic location of the terminal equipment of a user of publicly available telecommunications services) for marketing telecommunications services or for providing value-added services is permitted if the user (*ie,* subscriber or end user) gives his or her consent.

Location data

In order to use data about location (understood as location data beyond the data necessary for message transmission or billing), a provider of publicly available telecommunications services has to:

- Obtain the consent of the user to process data about location concerning this user, which may be withdrawn for a given period or in relation to a given call, or
- Anonymize this data.

A provider of publicly available telecommunications services is obliged to inform the user, prior to receiving its consent, about the type of data about location which is to be processed, about the purpose and time limits of the processing, and whether this data is to be passed on to another entity in order to provide a value-added service.

Processing data about location may only be performed by entities that:

- Are authorized by a public telecommunications network operator
- Are authorized by a provider of publicly available telecommunications services
- Provide a value-added service

Data about location may be processed only for purposes necessary to provide value-added services.

Cookies

The use and storage of cookies and similar technologies is only allowed on the condition that:

- The subscriber or the end user is directly informed in advance in an unambiguous, simple and understandable manner about:
- The purpose of storing and the manner of gaining access to this information
- The possibility to define the condition of the storing or the gaining of access to this information by using settings of the software installed on his or her telecommunications terminal equipment or service configuration
- The subscriber or end user, having obtained the information referred to above, gives his/her consent, and
- The stored information or the gaining of access to this information does not cause changes in the configuration of the subscriber's or end user's telecommunications terminal equipment or in the software installed on this equipment (the end user may grant consent by using the settings of the software installed in the final telecommunications device that he/she uses or by the service configuration)

The consent of the subscriber or end user is not required if storage or gaining access to cookies is necessary for:

- Transmitting a message using a public telecommunications network
- Delivering a service rendered electronically, as required by the subscriber or the end user

Entities providing telecommunications services or services by electronic means may install software on the subscriber's or end user's terminal equipment intended for using these services or use this software, provided that the subscriber or end user:

- Is directly informed, before the installation of the software, in an unambiguous, simple and understandable manner, about the purpose of installing this software and about the manner in which the service provider uses this software
- Is directly informed, in an unambiguous, simple and understandable manner, about the manner in which the software may be removed from the end user's or subscriber's terminal equipment
- Gives its consent to the installation and use of the software prior to its installation

According the current draft of the second act, the consent of the subscriber or the end user must comply with the GDPR requirements as regards the format. The legislative procedure is still ongoing and we will update you once the final version of the

amendments takes shape.

Enforcement and sanctions

A company that processes transmission data contrary to the Telecommunications Act or fails to meet obligations to obtain consent to process data about location or to store and to gain access to cookies may be subject to a fine of up to 3% of the company's revenues for the previous calendar year. The fine is imposed by the President of the OEC. In addition, the President of the OEC may impose a fine on a person holding a managerial position in the company (such as a member of the management board) of up to 300% of his or her monthly remuneration.

KEY CONTACTS

Ewa Kurowska-Tober
Partner, Head of IPT
T +48 22 540 74 1502
ewa.kurowska-tober@dlapiper.com

Lukasz Czynienik
Counsel
T +48 22 540 74 67
lukasz.czynienik@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

PORTUGAL

Last modified 11 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

Currently, processing of personal data in Portugal is mainly governed by the GDPR. The draft law for the implementation of the GDPR (Proposal of Law 120/XIII) is at Parliament for discussion and there is no final wording of it available at this stage. In accordance with the supervisory authority's position, the Personal Data Protection Law (Law 67/98, of 26 October (Personal Data Protection Law, as amended by Law no. 103/2015, of 24 August and enacted pursuant to Directive 95/46/EC) remains in force (*ie,* the provisions that do not contradict the GDPR), which may, potentially, creat some difficulties in the application of the new data protection legal regime until the entry into force of the GDPR implementation law.

Relevant data protection provisions in the context of electronic communications may also be found in Law 41/2004, of 18 August (Law on the processing of personal data and the protection of privacy in the electronic communications, as amended by Law 46/2012, of 29 August and enacted pursuant to Directive 2002/58/EC) (with subsequent amendments arising from Article 2 of Directive 2009/136/EC).

Although there is no final GDPR implementation law at this stage, the current position included in the Proposal of Law will be described without prejudice to subsequent amendments. According to the Proposal of Law, the same applies: (a) to the processing of personal data carried out in the national territory, regardless of the public or private nature of the controller or processor, even if the processing is carried out in compliance with legal obligations or for public interest

purposes, taking into account all the exclusions provided for in Article 2 GDPR; and (b) the processing of personal data carried out outside the national territory when: (i) it is carried out in the context of an activity of an establishment located in the national territory; or (ii) it concerns data subjects residing in the national territory, where the processing activities are subject to the provisions of Article 3(2) GDPR; or (iii) it affects data subjects who are Portuguese citizens that live abroad and whose data is registered at consular offices.

DEFINITIONS

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Personal Data Protection Law defines 'personal data' as any given information, in any format, including sound and image, related to a specific or an identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, namely by reference to a specific number or to one or more elements concerning his or her physical, physiological, mental, economic, cultural or social identity.

On the other hand, 'sensitive personal data' is considered to be any personal data revealing one's philosophical or political beliefs, political affiliations or trade union membership, religion, private life and racial or ethnic origin, and data concerning health or sex life, including genetic data.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Comissão Nacional de Proteção de Dados ('National Commission for the Protection of Data'. also known as 'CNPD').

Av. D. Carlos I, 134 - 1.°

1200-651 Lisboa

T +351 21 392 84 00

F +351 21 397 68 32

geral@cnpd.pt

www.cnpd.pt

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Under the prior Personal Data Protection Law, as a general rule, data controllers who process personal data should notify such activity to the supervisory authority (CNPD), unless a specific exemption applies. For instance, CNPD has issued decisions on the exemption of notification being applicable to activities related with salary processing, invoicing and client or supplier management, entry and exit of persons in buildings, among others. However, after the GDPR application date (*ie,* from May 25, 2018 onwards), in general terms, the need to notify of or obtain authorization for the processing activities is no longer applicable.

For certain categories of data (sensitive data, data regarding unlawful activities or criminal and administrative offenses or credit and solvability data) and certain types of processing, prior authorization from the CNPD is required, with any variations or changes to the processing of personal data determining mandatory amendment of the registration.

Notification is made electronically through CNPD's website by means of an official form including the following

information:

- Identity of the controller and its representative
- Purposes of the processing
- Third party entity responsible for the processing (data processor), if applicable
- Categories of entities to which the personal data is communicated, their identification and the purposes of communication if applicable
- All the personal data that will be processed, being necessary to indicate if sensitive data will be collected, as well as data concerning the suspicion of illegal activities, criminal or administrative offences and data regarding credit and solvability
- Grounds for lawful processing and a brief description of the data collection method used
- Storage period: the way of exercising the right of access and rectification
- Combination of personal data, if applicable
- Available means and methods for updating the data
- Any transfers of data to third countries, including a list of such entities and countries, what personal data is transferred, reasons and respective grounds for the transfer and the measures adopted in each transfer
- Physical and logical security measures implemented

It should be noted that, with the GDPR in force, these provisions will most likely be considered tacitly revoked, as they contradict the Regulation and namely one of its main principles: the principle of accountability.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Personal Data Protection Law did not provide for the requirement of appointing Data Protection Officers. Therefore, until the application date of the GDPR, organizations were not required to appoint a data protection officer.

However, after the GDPR application data, such appointment came to be required in the circumstances referred to above. According to the Proposal of Law: (a) the Data Protection Officer shall be designated based on professional qualities and expert knowledge of data protection law and practices and the ability to fulfill its legal tasks (a professional certification is not required for these purposes); (b) the controller or the processor shall designate a data protection officer in any case where the core activity: (i) consists of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (ii) consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

For the purposes of the mandatory notification of the data protection officer to the supervisory authority, in the context of Article 37 (7) of the GDPR, the supervisory authority established the applicable procedure for notification. A specific form made available by the supervisory authority on its website should be completed and submitted online (the form is available at https://www.cnpd.pt/DPO/DPOiniciar.aspx).

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous,*" and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)

- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to re-purpose personal data – *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new

purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise

of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision taking, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

1. Necessary for entering into or performing a contract
2. Authorized by EU or Member State law
3. The data subject has given their explicit (*ie,* opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Personal data may only be processed if any of the GDPR lawful bases apply.

Moreover, the data controller must provide the data subject with all the relevant processing information under the GDPR.

Regarding the processing of special categories of personal data and according to the Proposal of Law, in the cases provided for by Article 9(2)(h) and (i) GDPR (*ie,* where the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care of treatment or the management of health or social care systems or for reasons of public interest in the area of public health), the processing must be carried out by or under the responsibility of a professional who is subject to the obligation of secrecy, and appropriate information security measures must be ensured.

As concerns data subjects' rights, these shall follow GDPR requirements, with the Proposal of Law establishing that the right to data portability provided for in Article 20 of the GDPR only comprises the personal data provided by the respective data subjects and shall be provided, wherever possible, in an open format.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and

Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
d. The transfer is necessary for important reasons of public interest
e. The transfer is necessary for the establishment, exercise or defense of legal claims
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
g. The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State. A transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

As regards data transfers performed within the EU/EEA countries, mandatory notification to the Data Protection Authority (CNPD) is required and, in principle, data processing may commence immediately thereafter.

Transfers to non-EU/EEA countries or international organizations follow GDPR rules. In respect of transfers of personal data to third countries or international organizations, where the processing is necessary for compliance with a legal obligation and where it is carried out by public entities in the exercise of authority powers, the Proposal of Law establishes that said transfers shall be considered as in the public interest, as with the transfer of employee personal data.

Exceptionally, transfers performed under specific circumstances are possible, notably according to Standard Model Clauses or to Privacy Shield Framework holders. In such cases, data processing can be done, in principle, immediately after filing with CNPD.

CNPD has issued specific guidelines on IntraGroup Agreements (IGA) involving transfers of personal data to non-EU/EEA countries and considers that such transfers are always dependant on its prior authorisation (assessing if a determined IGA presents sufficient guarantees).

When IGA agreements follow EU model clauses, although designed for bilateral relationships, CNPD understands that there are grounds to authorize the transfers in an expedite manner if the data controller declares that such agreement is identical and in accordance with EU model clauses.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The security measures shall follow GDPR provisions. The proposal of Law also provides that health databases or centralised registers based on single platforms should meet the security and integrity requirements provided for by the GDPR.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Since the entry into force of the GDPR, personal data breach notifications are required in the circumstances provided in Article 33, GDPR. The supervisory authority set out the procedure for a personal data breach notification. A specific form on the supervisory authority's website should be completed and submitted only (the

form is available at https://www.cnpd.pt/DataBreach/).

Also Law 41/2004, of 18 August (as amended) establishes that companies that provide electronic communications services accessible to the public shall, without undue delay, notify the Data Protection Authority (CNPD) of a personal data breach. When the personal data breach may affect negatively the subscriber's or user's personal data, companies providing electronic communications services to the public should also, without undue delay, notify the breach to the subscriber or user so that they can take the necessary precautions.

For these purposes, a negative effect on personal data exists when the breach may result namely in theft or identity fraud, physical harm, significant humiliation or damage to reputation.

Additionally, if a person or entity is affected by a breach under the Personal Data Protection Law, he or she is entitled to file a claim to the CNPD or file a civil lawsuit to seek compensation for damages.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- Data subjects' rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The CNPD is the supervisory authority responsible for the enforcement of personal data protection laws and regulations in Portugal. Failure to comply with applicable data protection and privacy legal requirements may result in criminal, civil and administrative liability. The Proposal of Law establishes that:

(a) The use of personal data in a manner that is incompatible with the purposes of collection, unauthorized access, or deviation of personal data; the vitiation or erasure of personal data; the insertion of false data and the violation of the duty of secrecy, constitute crimes punishable by a prison sentence of up to four years or a fine of up to 480 days. In general terms, legal persons and similar entities have criminal liability.

(b) Any person who has suffered damages due to the unlawful processing of personal data or any other act that violates the provisions of the GDPR or of the national law on personal data protection, has the right to compensation from the data controller or the processor for the damage suffered.

(c) Very serious administrative offences shall be punishable with a fine:

- From EUR 5,000 to EUR 20,000,000 or 4% of the total worldwide annual turnover, whichever is higher, in the cases of large companies
- From EUR 2,000 to EUR 2,000,000 or 4% of the total worldwide annual turnover, whichever is higher, in the case of SMEs
- From EUR 1,000 to EUR 500,000, in the case of natural persons

Serious administrative offences shall be punishable with a fine:

- From EUR 2,500 to EUR 10,000,000 or 2% of the total worldwide annual turnover, whichever is higher, in the cases of large companies
- From EUR 1,000 to EUR 1,000,000 or 2% of the total worldwide annual turnover, whichever is higher, in the cases of SMEs
- From EUR 500 to EUR 250,000, in the case of natural persons

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

As established under Law 41/2004, of 18 August (as amended), sending unrequested communications for direct marketing purposes to natural persons is subject to express prior consent of the subscriber or user (that is, the opt-in rule applies). This includes use of automated calling and communications that do not rely on human intervention automatic call devices, fax or electronic mail, including SMS, EMS, MMS and other similar applications.

As regards direct marketing communications to legal persons, these are allowed insofar as opt-out is offered. Legal persons may refuse future communications and request registration in the non-subscribers list.

This does not prevent the supplier that has obtained its clients' data and contacts in connection with the sale of a product or service to use such data for direct marketing of its own products or services or products or services similar to the ones provided.

Nevertheless, the supplier shall ensure that these clients are given the opportunity to object to the use of such data, free of charge, clearly and explicitly, and in an easy manner, at the time of the respective collection, and on each message (when the client did not opt-out initially upon collection of the data).

Moreover, sending electronic mail for direct marketing purposes via email where the identity of the sender is disguised or concealed, as well as where there is no valid means of contact to send a request to stop these communications or encouraging recipients to visit websites that violate these rules is strictly forbidden.

ONLINE PRIVACY

Cookie compliance

As determined by Law 41/2004, of 18 August, storage of data and the possibility of accessing data stored in a subscriber or user terminal is only allowed if the subscriber or user has provided prior consent. Such consent must be based on clear and comprehensive information.

This does not prevent technical storage or access for the sole purpose transmitting communications over an electronic communication network, if strictly necessary for the provision of a service expressly requested by the subscriber or user.

Traffic Data

Traffic data must be erased or anonymized when no longer needed for the transmission of communications. Processing of traffic data requires prior express consent and the user or subscriber shall be given the possibility to remove it at any time. Such processing may only be carried out to the extent and for the time strictly necessary for the sale of electronic communications services or the provision of other value-added services.

Processing of traffic data is admissible when required for billing and payment and only until the end of the period during which the bill may lawfully be challenged or payment pursued.

Complete and accurate information on the type of data being processed must be provided, as well as the processing purposes and duration and the possibility of disclosure to third parties for the provision of value added services.
Processing should be limited to workers or employees in charge of billing or traffic management, customer inquiries, fraud detection, sale of electronic communications services accessible to the public, or the provision of value added services, as well as to the strictly necessary information for the purposes of carrying out such activities.

Location Data

Processing of location data is allowed only if such data is anonymized or to the extent and for the time necessary for the provision of value added services, provided that prior express consent was obtained. Prior information to the data subjects must also be provided.

Companies must ensure there is an option to withdraw consent at any time, or to temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication, in a simple manner and free of charge.
Non-compliance with these opt-in rules is considered an administrative offence, punishable with fines ranging from EUR 5,000 to EUR 5,000,000.

KEY CONTACTS

Joao Costa Quinta
Partner
T +351 213 583 620
Joao.Quinta@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

QATAR

Last modified 28 January 2019

LAW

Note: Please also see Qatar — Financial Center Free Zone.

This overview is based on an unofficial English translation of the Law No. (13) of 2016 Concerning Personal Data Protection. The Qatar government does not issue official English translations of the laws of the State of Qatar.

Qatar has implemented Law No. (13) of 2016 Concerning Personal Data Protection ("the Data Protection Law").

With its Data Protection Law—adopted in 2016—Qatar became the first Gulf Cooperation Council (GCC) member state to issue a generally applicable data protection law.

While the Data Protection Law took effect in 2017, executive regulations further implementing this law are expected to be passed in 2019.

The Data Protection Law applies to personal data when this data is any of the following:

- Processed electronically
- Obtained, collected or extracted in any other way in preparation for electronic processing
- Processed by combining electronic processing and traditional processing

The Data Protection Law provides that each individual shall have the right to privacy of their personal data. Such data may only be processed within a framework of transparency, honesty, respect for human dignity and in accordance with the provisions of the Data Protection Law.

DEFINITIONS

Definition of personal data

Personal data is defined under the Data Protection Law as data relating to a natural person whose identity is identified or is reasonably identifiable, whether through this data or by means of combining this data with any other data or details.

Definition of sensitive personal data

Sensitive personal data means personal data consisting of information as to a natural person's:

- Ethnic origin
- Health
- Physical or mental health or condition
- Religious beliefs
- Relationships
- Criminal records

NATIONAL DATA PROTECTION AUTHORITY

Qatar Ministry of Transport and Communications (MoTC).

REGISTRATION

There is currently no requirement in Qatar for data controllers who process personal information to register with the regulator, the MoTC.

DATA PROTECTION OFFICERS

There is currently no obligation for organizations in Qatar to appoint a data protection officer. There is an obligation on the data controller to specify processors responsible for protecting personal data, train them appropriately on the protection of personal data and raise their awareness in relation to protecting personal data.

COLLECTION & PROCESSING

Generally, data subject consent is required to collect and process personal data, except to the extent processing is deemed necessary for a lawful purpose of the controller, or the third party to whom the personal data is sent.

Lawful purpose is defined in the Data Protection Law as "the purpose for which the personal data of the data subject is being processed in accordance with the law," which includes specific purposes set forth under Data Protection Law as described below.

Prior to processing personal data, the data controller must notify the data subject of the following information:

- The details of the data controller or another party who processes the data on behalf of the data controller
- The lawful purpose for which the data controller or any third party wants to process the personal data
- A comprehensive and accurate description of the processing activities and the degrees of disclosure of personal data for the lawful purpose
- Any other information deemed necessary and required for the satisfaction of personal data processing

The data controller is free to process data without the consent of the data subject or a lawful purpose in the following circumstances:

- The data processing is in the public interest
- The data processing is required to meet a legal obligation
- The data processing is required to protect the data subjects vital interests
- The data processing is required for scientific research being conducted in the public interest
- The data processing is required to investigate a crime, if officially requested by the investigating authorities

Sensitive personal data may not be processed except after obtaining authorization from the MoTC. The procedure for obtaining this authorization has not yet been issued (this is likely to be in the form of a Ministerial resolution).

TRANSFER

Data controllers may collect, process and transfer personal data when the data subject consents, unless deemed necessary for realizing a 'lawful purpose' for the controller or for the third party to whom the personal data is sent. The data controller has to demonstrate, when disclosing and transferring personal data to the data processor, that the transfer is for a lawful purpose and that the transfer of data is made pursuant to the provisions of the Data Protection Law.

Data controllers should not take measures or adopt procedures that may curb trans-border data flow, unless processing such data violates the provisions of the Data Protection Law or will cause gross damage to the data subject. The Data Protection Law defines 'trans-border data flow' as accessing, viewing, retrieving, using or storing personal data without the constraints of state borders.

SECURITY

Data controllers must take appropriate technical and organizational measures to securely manage personal data.

The data controller must carry out the following procedures:

- Review privacy protection procedures before implementing new processing operations
- Specify the processors responsible for protecting the personal data
- Train processors on the protection of personal data and raise their awareness relating to the same
- Set up internal systems to receive and investigate complaints, data access requests, data correction or deletion requests and provide the data subjects with information relating to the same
- Set up internal systems for the effective management of personal data, and report any violation of the same with the aim of safeguarding personal data
- Adopt suitable technical means to enable individuals to exercise their rights to access, review and correct their personal data directly
- Carry out comprehensive review and checking of the commitment to protect personal data
- Verify that the data processor abides by the instructions given to him/her or take suitable precautions to protect personal data, and continually monitor that situation

The data controller and processor must take necessary precautions to protect personal data against loss, damage, amendment, disclosure or access thereto or use thereof in an accidental or unlawful way. The Data Protection Law states the precautions taken must be proportionate to the nature and importance of the personal data to be protected. Organizations should adopt best practice methodologies in keeping with their business sector.

BREACH NOTIFICATION

There is an obligation on the data controller to notify the regulator, the MoTC and the data subject of any breaches of the measures to protect the data subject's privacy if it is likely to cause damage to the data subject.

ENFORCEMENT

In Qatar, the MoTC is responsible for the enforcement of the Data Protection Law. Any data subject may submit a complaint to the MoTC in the case of a violation of the Data Protection Law. The MoTC will investigate the complaint and, if the complaint is found to be valid, the MoTC can oblige the data controller or processor to rectify the violation within a specified time period.

The MoTC can also impose fines of up to ﷼5 million (US$1.4 million) for violations of the Data Protection Law.

ELECTRONIC MARKETING

Unsolicited direct marketing is prohibited under the Data Protection Law, which requires prior consent to send electronic marketing communications (including by wired or wireless communication).

All electronic marketing communications must include the identity of the sender and an indication that it is sent for the purpose of direct marketing. The message must include an address that can easily be reached and must enable the recipient to send a message requesting the sender to stop the electronic communication and enable the recipient to withdraw the consent at any time.

ONLINE PRIVACY

The Data Protection Law (or any other law) does not specifically regulate online privacy or the use of cookies and location data except in relation to children. Owners and operators of websites must observe the followings requirements:

- Place a notification on the website regarding how children's data is used and its disclosure policies
- Obtain express approval from the parents or guardian of the child before processing any personal data
- Provide the child's parent or guardian—upon request and after verifying the identity of the child's parent or guardian—a description of the personal data that is being processed, stating the purpose of the processing, and a copy of the child's data that is being collected and processed
- Delete, erase, or suspend the processing of any personal data that was collected from the child or about the child, if the child's parent or guardian requests this, and
- Refrain from making any child's participation in a game or prize offer, or any other activity conditional on the child's submission of personal data which goes beyond what is required for the purposes of participation in the game or prize offer

KEY CONTACTS

Brenda Hill
Legal Director
T +974 4420 6126
brenda.hill@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

QATAR - FINANCIAL CENTRE FREE ZONE

Last modified 28 January 2019

LAW

Note: Please also see Qatar.

The Qatar Financial Centre (QFC) implemented QFC Regulation No. 6 of 2005 on QFC Data Protection Regulations (DPL).

Additionally, under the powers granted to the QFC Authority under Article 21 of the DPL, the QFC Authority has issued the Data Protection Rules 2005 (DPR).

DEFINITIONS

Definition of data controller

Any person in the QFC who alone or jointly with others determines the purposes and means of the processing of personal data.

Definition of data processor

Any person who processes personal data on behalf of a data controller.

Definition of Identifiable Natural Person

Is a natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

Definition of personal data

Any information relating to an identified natural person or an identifiable natural person.

Definition of processing

Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Definition of sensitive personal data

Personal data revealing or relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and health or sex life.

NATIONAL DATA PROTECTION AUTHORITY

The Employment Standards Office at the QFC Authority is effectively the administrator of the DPL and DPR in the QFC.

Employment Standards Office
Qatar Financial Centre
Level 8, QFC Tower 1
Westbay
Doha, Qatar
eso@qfc.qa
Tel: +974 44967609

REGISTRATION

Unless certain exceptions apply, data controllers must obtain a permit from and provide notice to the QFC Authority prior to processing sensitive personal data or transferring personal data outside of the QFC to a recipient who is not subject to laws or regulations that ensure an adequate level of protection for that personal data.

DATA PROTECTION OFFICERS

There is no requirement under the DPL or the DPR for organizations to appoint a data protection officer. Though note the general obligation of a data controller to implement appropriate technical and organizational measures to protect personal data, as further detailed below (see Security section). It is however recommended that organizations that operates on a large scale or carries out regular and systematic monitoring of individuals appoint an individual responsible for overseeing the data controller's compliance with data protection requirements.

COLLECTION & PROCESSING

Data controllers may process personal data when any of the following conditions are met:

- The data subject has given his/her unambiguous consent to the processing of that personal data (DPL, Article 7(1))
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (DPL, Article 7(2))
- Processing is necessary for compliance with any legal obligation to which the data controller is subject (DPL, Article 7(3))
- Processing is necessary in order to protect the vital interests of the data subject (DPL, Article 7(4))
- Processing is necessary for the performance of a task carried out in the interests of the QFC, or in the exercise of the QFC Authority, the QFC Regulatory Authority, the QFC Tribunal or Appeals Body functions or powers vested in the data controller or in a third party to whom the personal data is disclosed (DPL, Article 7(5)), or
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the personal data is disclosed, except where such interests are overridden by compelling legitimate interests of the data subject relating to the data subject's particular situation (DPL, Article 7(6))

Data controllers may process sensitive personal data when any of the following conditions are met:

- The data subject has given his/her explicit consent to the processing of that personal data (DPL, Article 8(1)(A))
- Processing is necessary for the purposes of carrying out the obligations and specific rights of the data controller in the field of employment law (DPL, Article 8(1)(B))
- Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his/her consent (DPL, Article 8(1)(C))
- Processing is carried out by a foundation, association or any other nonprofit-seeking body in the course of its legitimate activities with appropriate guarantees that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed to a third party without the consent of the data subjects (DPL, Article 8(1)(D))
- The processing relates to personal data which is manifestly made public by the data subject or is necessary for the

establishment, exercise or defense of legal claims (DPL, Article 8(1)(E))
- Processing is necessary for compliance with any legal obligation to which the data controller is subject (DPL, Article 8(1)(F))
- Processing is necessary to uphold the legitimate interests of the data controller recognized in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by compelling legitimate interests of the data subject relating to the data subject's particular situation (DPL, Article 8(1)(G))
- Processing is necessary to comply with auditing, accounting or anti-money laundering obligations that apply to a data controller (DPL, Article 8(1)(H)), or
- Processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where that personal data is processed by a health professional subject under national laws or regulations established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy (DPL, Article 8(1)(I))

TRANSFER

Data controllers may transfer personal data out of the QFC if the personal data is being transferred to a Recipient in a jurisdiction that has laws and regulations that ensure an adequate level of protection for that personal data (DPL, Article 9(1)). The adequacy of the level of protection ensured by laws and regulations to which the Recipient is subject to shall be assessed in light of all the circumstances surrounding a personal data transfer operation or set of personal data transfer operations, including but not limited to:

- The nature of the data
- The purpose and duration of the proposed processing operation or operations
- If the data does not emanate from the QFC, the country of origin and country of final destination of the personal data
- Any relevant laws to which the recipient is subject, including processional rules and security measures

In the absence of an adequate level of protection, data controllers may transfer personal data out of the QFC if any of the following are true:

- QFC Authority has granted a permit for the transfer or the set of transfers and the data controller applies adequate safeguards with respect to the protection of this personal data (DPL Article 10(1)(A)). Article 3.2 of the DPR then sets out the requirements for applying for such a permit (including a description of the proposed transfer of personal data for which the permit is being sought and including a description of the nature of the personal data involved)
- Data subject has given his / her unambiguous consent to the proposed transfer (DPL, Article 10(1)(B))
- Transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken in response to the data subject's request (DPL, Article 10(1)(C))
- Transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party (DPL, Article 10(1)(D))
- Transfer is necessary or legally required on grounds important in the interests of the QFC, or for the establishment, exercise or defense of legal claims (DPL, Article 10(1)(E))
- Transfer is necessary in order to protect the vital interests of the data subject (DPL, Article 10(1)(F))
- Transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case (DPL, Article 10(1)(G))
- Transfer is necessary for compliance with any legal obligation to which the data controller is subject (DPL, Article 10(1)(H))
- Transfer is necessary to uphold the legitimate interests of the data controller recognized in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by legitimate interests of the data subject relating to the data subject's particular situation (DPL, Article 10(1)(I))
- Transfer is necessary to comply with auditing, accounting or anti-money laundering obligations that apply to a data controller which is established in the QFC (DPL, Article 10(1)(J))

Authorities who receive personal data in the context of a particular inquiry are not regarded as Recipients under the DPL or the DPRs (as per the definition of Recipient in the DPL).

SECURITY

Data controllers must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing, in particular where sensitive personal data is being processed or where the personal data is being transferred out of the QFC to a jurisdiction without an adequate level of protection (DPL, Article 14(1)).

When applying for a permit to process sensitive personal data, or transfer personal data out of the QFC to a jurisdiction without an adequate level of protection, data controllers must include detail regarding the safeguards employed to ensure the security of such sensitive personal data/personal data (respectively, Articles 2.1.1(l) and 3.2.1(l) of the DPR).

The measures implemented ought to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected (DPL, Article 14(2)).

BREACH NOTIFICATION

There is no requirement under the DPL and nor the DPR to inform the QFC Authority of any breaches of personal data databases. It is nevertheless recommended that a data controller notifies the QFC Authority and the concerned data subjects of events of breach as soon as practicable and in any event, within 72 hours from the time the data controller becomes aware of such breach.

ENFORCEMENT

In the QFC, the ESO oversees the enforcement of the DPL.

If the QFC Authority is satisfied that a data controller has contravened or is contravening the DPL or DPR, the QFC Authority may issue a direction to the data controller requiring it to do either or both of the following:

- To do or refrain from doing any act or thing within such time as may be specified in the direction (DPL, Article 22(1)(A))
- To refrain from processing any personal data specified in the direction or to refrain from processing personal data for a purpose or in a manner specified in the direction (DPL, Article 22(1)(B))

A data controller may file an appeal against a decision by the QFC Authority to issue a direction pursuant to DPL, Article 22(1) at the QFC Tribunal (DPL, Article 22(3)).

ELECTRONIC MARKETING

Immediately upon collecting personal data, the DPL requires data controllers to provide data subjects who they have collected personal data from, with, among other things, any further information to the extent necessary (having regard to the specific circumstances in which the personal data is collected). This includes information on whether the personal data will be used for direct marketing purposes (DPL, Article 11).

If the personal data has not been obtained from the data subject, the data controller or their representative must at the time of undertaking the recording of personal data – or if it is envisaged that the personal data will be disclosed to a third party, no later than when the personal data is first recorded or disclosed – provide the data subject with, among other things, information regarding whether the personal data will be used for direct marketing purposes (DPL, Article 12).

Before personal data is disclosed for the first time to third parties or used on a data subject's behalf for the purposes of direct marketing, data subjects also have the right to be informed and to be expressly offered the right to object to such disclosures or uses (DPL, Article 16(1)(B)).

Additionally, the DPL requires a data controller to record various types of information regarding its personal data processing

operations (Article 17(1) and 2(A)). This must include an explanation of the purpose for the personal data processing (DPR, Article 4(1)(B)). The DPR suggests that one of these purposes may be for advertising, marketing and public relations for the data controller itself or for others (Article 4.1(e)).

ONLINE PRIVACY

The DPL or DPR do not contain specific provisions relating to online privacy, however, the broad provisions detailed above are likely to apply. In addition, as Qatar criminal law applies in the QFC, the privacy principles laid out therein may apply (see Qatar).

KEY CONTACTS

Brenda Hill
Legal Director
T +974 4420 6126
brenda.hill@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ROMANIA

Last modified 10 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A regulation (unlike the directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An establishment may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extraterritorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "to the offering of goods or services" (no payment is required) to such data subjects in the EU or "the monitoring of their behaviour" as far as their behaviour takes place within the EU.

Law no. 190/2018 on the measures for the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("Law no. 190/2018") was published in the Official Gazette no. 651/26.07.2018 and became applicable on July 31, 2018.

Law no. 190/2018 regulates, among others, the following activities, in addition to providing a framework related to the sanctions applicable to public authorities and public bodies:

- Processing of genetic data, biometric data or health data
- Processing of a national identification number
- Processing of personal data in the context of employment relationships
- Processing of personal data and of special categories of personal data within the performance of a task carried out in the public interest

DEFINITIONS

Personal data is defined as "any information relating to an identified or identifiable natural person." A low bar is set for identifiable – if the natural person can be identified using "all means reasonably likely to be used" the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences.**

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "alone or jointly with others, determines the purposes and means of the processing of personal data." The processor "processes personal data on behalf of the controller," acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The **data subject** is a living, natural person whose personal data are processed by either a controller or a processor.

Law no. 190/2018 does not provide any specific definitions with respect to personal data, as this is defined by the GDPR. However, the following relevant definitions are included:

- "Public authorities and bodies" means the Chamber of Deputies and the Senate, the Presidential Administration, the Government, the ministries, other specialized bodies of the central public administration, autonomous public authorities and institutions, local and county public administration authorities, other public authorities, as well as any institutions subordinated / coordinated by such authorities. Religious establishments, organisations and foundations of public service are considered public authorities / bodies.
- "National identification number" means the number by which an individual is identified in certain record systems and which has general applicability, such as: (i) personal identification number, (ii) serial number and identity card number, (iii) passport number, (iv) driving license, and the (v) social health insurance number.
- "Remediation plan" means an annex to the report for finding and sanctioning misdemeanours, drafted by the National Supervisory Authority for Personal Data Processing (hereinafter referred to as ANSPDCP) setting remediation measures and terms.
- "Remediation measure" means a solution imposed by ANSPDCP in the remediation plan, in view of ensuring the compliance of the public authority/body with the obligations provided by the law.
- "Remediation term" means the time period comprised between 60 and 180 days, calculated from the moment when the report for finding and sanctioning misdemeanours is communicated, in which the public authority/body may undertake remedial actions in order to correct any irregularities assessed by ANSPDCP and comply with its legal obligations.

All definitions included by the GDPR in Article 4 are applicable and have the same meaning as in Law no. 190/2018.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (similar to the CNIL in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the GDPR.

The GDPR creates the concept of "**lead supervisory authority**." Where there is cross-border processing of personal data (*ie*

, processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by, and answer to, the supervisory authority for their main or single establishment, the so-called "lead supervisory authority."

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory. ead supervisory authority is therefore of somewhat limited use to multinationals.

The National Supervisory Authority For Personal Data Processing
(in Romanian 'Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal' or 'ANSPDCP')
28 30 Magheru Blvd
District 1, Bucharest
T +40 318 059 211
F +40 318 059 602
www.dataprotection.ro

REGISTRATION

There are no EU-wide systems of registration or notification, and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority.

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities, which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

All obligations in respect of notifying ANSPDCP of the processing of personal data were repealed on May 25, 2018 (when GDPR came into force).

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer (DPO) if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities, provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have *expert knowledge* of data protection law and practices, though it is possible to outsource the DPO role to a service provider.

Controllers and processors are required to ensure that the DPO is involved "properly and in a timely manner in all issues which relate to the protection of personal data," and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks.

The specific tasks of the DPO, set out in GDPR, include:

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

In addition to the requirements provided by the GDPR in Articles 37 to 39, Law no. 190/2018 provides that a data protection officer (DPO) must be designated whenever the entity acting as controller is processing a national identification number, including by collecting or disclosing any documents enclosing such national identification number, when the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, in accordance with the provisions of Article 6 paragraph 1 letter (f) of the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be:

- Processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle")
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle")
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- Accurate and where necessary kept up to date (the "accuracy principle")
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle")
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle")

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance for potentially years after a particular decision relating to processing personal data was rendered. Record-keeping, auditing and appropriate governance will all play a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "freely given, specific, informed and unambiguous," and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of

the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited, except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law.

Processing for a Secondary Purpose

Increasingly, organisations wish to re-purpose personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected. These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)

- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymisation

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, that is, the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language.

The following information must be provided at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten')

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the

search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg*, commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling

Automated decision making (including profiling) "which produces legal effects concerning [the data subject] … or similarly significantly affects him or her" is only permitted where:

- Necessary for entering into or performing a contract
- Authorized by EU or Member State law
- The data subject has given their explicit (*ie*, opt-in) consent

Further, where significant automated decisions are taken on the basis of first or third grounds above, the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

1. Processing of genetic data, biometric data or health data - The processing of genetic, biometric or health data for the purpose of achieving an automated decision-making process or for profiling purposes is permitted only with the explicit consent of the data subject or if the processing is performed based on express legal requirements, with the obligation of the controller to implement adequate measures for the protection of the rights, freedoms and legitimate interests of the data subject. Law no. 190/2018 does not specify or provide any examples with respect to what type of measures should be implemented by the controller in view of the processing.

Law no. 190/2018 expressly allows the processing of health data for the purpose of public health, as defined under Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work. However, subsequent processing of such data may not be performed for other purposes and by third parties.

2. Processing a national identification number - Law no. 190/2018 provides that processing of a national identification

number, including by collecting or disclosing any documents enclosing such national identification number, may be carried out in the situations provided for in Article 6 (1) of the GDPR. However, where processing is based on the legitimate interests pursued by the controller or by a third party (i.e. Article 6 (1) (f) of the GDPR), the processing activities may be carried out only if the following guarantees have been implemented by the controller:

a. Adequate technical and organizational measures to observe, in particular, the principle of data minimization and to ensure the security and confidentiality of personal data processing, according to the provisions of art. 32 of the GDPR
b. The appointment of a DPO
c. Establishment of a retention policy in accordance with the nature of the personal data and the purpose of the processing, as well as specific deadlines in which personal data must be deleted or revised for deletion
d. Regular training of the personnel that handles personal data processing activities

3. Processing of personal data in the context of employment relationships - The electronic monitoring and / or video surveillance systems of employees at the workplace based on the legitimate interests of the employer is permitted only if the following apply:

a. The legitimate interests pursued by the employer are thoroughly justified and prevail over the interests or rights and freedoms of the data subjects.
b. The employer has made the compulsory, complete and explicit prior information to the employees.
c. The employer consulted the relevant trade union or, where applicable, the employees' representatives prior to the introduction of the monitoring systems.
d. Other less intrusive forms and ways to achieve the goal pursued by the employer have not previously proved their effectiveness.
e. The retention duration of personal data is proportional to the purpose of processing, but not more than 30 days, except for situations expressly governed by law or in duly justified cases.

4. Processing of personal data for journalistic purposes or for the purpose of academic, artistic or literary expression - According to Law no. 190/2018, in view of ensuring a balance between the right to personal data protection, freedom of expression and the right to information, processing of personal data for journalistic purposes, or for the purposes of academic, artistic or literary expression may be performed if such processing refers to personal data which were manifestly made public by the data subject or which are strongly connected to the quality of public person of the data subject or to the public nature of the facts in which the data subject is involved, by derogation from the following chapters of the GDPR:

a. Chapter II - Principles
b. Chapter III - Rights of the data subject
c. Chapter IV - Controller and processor
d. Chapter V - Transfers of personal data to third countries or international organizations
e. Chapter VI - Independent supervisory authorities
f. Chapter VII - Cooperation and consistency
g. Chapter IX - Provisions relating to specific processing situations

5. Processing of personal data for scientific or historical research purposes, statistical purposes or archiving in the public interest purposes - According to Law no. 190/2018 Articles 15, 16, 18 and 21 of the GDPR do not apply in case personal data are processed for scientific or historical research purposes, to the extent the rights mentioned in these Articles are likely to render impossible or seriously impair the achievement of the objectives of the processing, and such derogations are necessary for achieving such objectives. These derogations are applied only with respect to archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and not with respect to other purposes for which the personal data may be used. Articles 15, 16, 18, 19, 20 and 21 GDPR do not apply in cases where personal data

is processed for archiving purposes in the public interest to the extent that the rights mentioned in those Articles are likely to render impossible or seriously impair the achievement of the objectives of the processing, and such derogations are necessary for achieving such objectives.

These derogations are applicable only with respect to scientific or historical research purposes and for archiving in the public interest purposes, and not with respect to other purposes for which the personal data may be used. These derogations are applicable only if appropriate safeguards for the rights and freedoms of data subjects are implemented, in accordance with Article 89(1) GDPR.

TRANSFER

Transfers of personal data by a controller or a processor to countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted when certain conditions are met.

The European Commission has the power to make an adequacy decision in respect of non-EU countries, determining that it provides for an adequate level of data protection, and thereby permitting personal data to be freely transferred to that country. Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes, among other things, binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where any of the following apply:

- Explicit informed consent has been obtained
- The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
- The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
- The transfer is necessary for important reasons of public interest
- The transfer is necessary for the establishment, exercise or defence of legal claims
- The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
- The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

No specific provisions / derogations are provided by Law no. 190/2018 with respect to personal data transfers.

SECURITY

The GDPR does not prescribe specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A one-size-fits-all approach is therefore the antithesis of this requirement.

However, the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

- The pseudonymization and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

No specific provisions / derogations are provided by Law no. 190/2018 with respect to the security measures to be undertaken by controllers / processors.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay.

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach.

The notification to the supervisory authority must include where possible:

- The categories and approximate numbers of individuals and records concerned
- The name of the organisation's data protection officer or other contact
- The likely consequences of the breach and the measures taken to mitigate harm

Controllers are also required to keep a record of all data breaches (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

No specific provisions / derogations are provided by the Law no. 190/2018 with respect to the notification of a personal data security breach. However, where data controllers notify a personal data breach to ANSPDCP, a special notification form must be filled out and submitted.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or €20 million (whichever is higher).

The European Commission intends that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that undertaking should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define undertaking and the case law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of undertaking. Under EU competition law case law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on subsidiaries in some circumstances (broadly where there is participation or control), under a theory so-called look through liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories. The highest fines of up to €20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of any of the following:

- The basic principles for processing including conditions for consent
- Data subjects' rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines of up to €10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of any of the following:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines, but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive.

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered material or non-material damage as a result of a breach of the GDPR has the right to receive compensation from the controller or processor. The inclusion of non-material damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf.

Individuals also enjoy the right to lodge a complaint with a supervisory authority.

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision.

Data subjects enjoy the right to an effective legal remedy against a controller or processor.

ANSPDCD is entitled to investigate any breach of the GDPR provisions *ex officio* or following a complaint filed by a prejudiced data subject. The procedure on how ANSPDCP investigations can be conducted is provided by ANSPDCP Decision no. 161/2018.

Law no. 190/2018 provides specific rules with respect to enforcement. Specifically, ANSPDCP may issue written warnings and apply fines.

Misdemeanours committed by public authorities / bodies, can be sanctioned with a fine ranging between RON10,000 (€2,100) to RON200,000 (€43,000).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time.

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC ("ePrivacy Directive"), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced by references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The processing of personal data for electronic marketing purposes is regulated under Law no. 506/2004, on the processing of personal data in the electronic communications sector implementing Directive 2002/58/CE ("Law 506/2004"). According to this law, it is forbidden to send commercial communications by using automatic call systems that do not require the intervention of a human operator, by fax or electronic mail or any other method employing publicly available electronic communications services, except where the subscriber or user of a publicly electronic communications service has expressly consented in advance to receive such communications.

However, in cases where a natural or legal person has directly obtained the email address of a client upon the sale or provision of a product or service, the natural or legal person may use the respective address for the purpose of sending commercial communications regarding similar products or services, provided that clients are clearly and expressly offered the possibility to oppose by way of an easily accessible and free-of-charge method, not only when the email address is collected but also with each commercial communication received, in a case where the customer has not initially objected.

ONLINE PRIVACY

The processing of traffic data, location data and the implementation of cookies is regulated under Law 506/2004.

Traffic data

Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication, but no later than three years from the date of such a communication. However, traffic data may be retained for the purpose of marketing the services offered to data subjects, or in view of the provision of value-added services, solely throughout the marketing period and provided that data subjects have previously consented to the processing of traffic data. The processing of traffic data for billing purposes or the establishment of payment obligations for interconnection is permitted solely for a period of three years following the due date of the respective payment obligation. The processing of traffic data for the establishment of contractual obligations of the communication services subscribers, with payment in advance, is permitted solely for a period of three years following the date of the communication. Data subjects may withdraw their consent at any time. The provider of electronic communication services must inform data subjects in respect of the processed traffic data, and the duration of processing, prior to obtaining their consent.

Communication service providers and entities acting under their authority may process traffic data for:

- Management of billing and traffic
- Dealing with enquiries of data subjects
- Prevention of fraud, or
- The provision of communication services or value added services, and is permitted only if it is necessary to fulfil such purpose

Location data

The processing of location data is permitted when:

- Data is rendered anonymous
- Data subjects have consented to such processing for the duration necessary for the performance of value added services, or
- The purpose of the value-added service is the unidirectional and nondifferentiated transmission of information towards users

The service provider must inform the users or subscribers, prior to obtaining their consent, in respect of the type of location data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent at any time.

Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, communication service providers must grant users the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

Cookies

The storing of cookies on user terminals is permitted, subject to the following cumulative conditions:

- Users have expressly consented thereto (Law 506/2004 also provides that consent may be given by way of browser settings or other similar technologies)
- The information requirements provided by Data Protection Law have been complied with in a clear and user-friendly manner, to include references regarding the purpose of processing of the information stored by users

Should the service provider allow the storing of third-party cookies within a user's computer terminal, they will have to be informed about the purpose of such processing and the manner in which browser settings may be adjusted in order to refuse third-party cookies.

Consent is not required where cookies are:

- Used for the sole purpose of carrying out the transmission of a communication over an electronic communications

network, or

- Strictly necessary for the provision of an information service expressly requested by the subscriber or the user

Failure to comply with the requirements of Law 506/2004 is classified as a minor offence and is sanctionable with fines ranging from €1,120 to €22,500. In the case of companies whose turnover exceeds approximately €1.12 million, the amount of fines may reach up to 2% of the respective company's turnover. Upon request of the courts of law, of the criminal prosecution authorities or of the authorities competent in the area of national defence and security with the prior approval of the judge, providers of electronic communication services offered to the public and providers of electronic communication public networks shall make available, as soon as possible, but no later than 48 hours, traffic data, data regarding user terminals, as well as geolocation data.

KEY CONTACTS

Ana-Maria Andronic
Head of Intellectual Property and Technology
T +40 372 155 816
anamaria.andronic@dlapiper.com

Flavius Florea
Managing Associate
T +40372155829
flavius.florea@dlapiper.com

Corina Badiceanu
Associate
T +40372155853
corina.badiceanu@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

RUSSIA

Last modified 24 January 2018

LAW

Fundamental provisions of data protection law in Russia can be found in the Russian Constitution, international treaties and specific laws. Russia is a member of the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention) (ratified by Russia in 2006) and the Russian Constitution establishes the right to privacy of each individual (articles. 23 and 24). Most rules are found in specific legislation, particularly the Data Protection Act No. 152 FZ dated 27 July 2006 (DPA) and various regulatory acts adopted to implement the DPA as well as other laws, including the Information, Information Technologies and Information Protection Act No. 149 FZ dated 27 July 2006 establishing basic rules as to the information in general and its protection. In addition, the Russian Labour Code contains provisions on the protection of employees' personal data (Part XIV). Other laws may also contain data protection provisions which implement the provisions of DPA in relation to specific areas of state services or industries.

On 22 July 2014 notable amendments to the DPA were adopted and came into force on 1 September 2015. The amendments require all personal data operators to store and process any personal data of Russian individuals within databases located in Russia (subject to few exceptions). The penalty for violation of this requirement is ultimately the blocking of websites involving unlawful handling of Russian personal data. A Register of Infringers of Rights of Personal Data Subjects shall be established by the *Roscomnadzor* and from there and the *Roscomnadzor* may move to block websites.

As the amendments are newly passed and a track record of enforcement and legal interpretation has not been established, it is still unclear as to how this register and the website blocking would work in practice. According to clarifications of Russian regulators, storing and processing of personal data of Russian individuals outside of Russia can still be compliant with the law as long as primary (often interpreted as initial) storage and processing of data is done in Russia. It is still an open question whether keeping "mirror" databases in Russia and elsewhere would be deemed as compliant.

DEFINITIONS

Definition of personal data

Personal data is defined in law as any information that relates directly or indirectly to the specific or defined physical person (the data subject). This can be widely interpreted in various contexts, so it is important to consider each situation carefully.

Definition of sensitive personal data

Sensitive personal data is defined as special categories of personal data in Russian legislation. Such special categories include data related to race, national identity, political opinions, religious and philosophical beliefs, health state, intimacies and biometrical data.

NATIONAL DATA PROTECTION AUTHORITY

Federal Service for Supervision of Communications, Information Technologies and Mass Media or, in short, *Roscomnadzor*

('Agency')

Build. 2, 7, Kitaigorodskiy proezd
Moscow, 109074

T +7 495 987 6800
F +7 495 987 6801

http://www.rsoc.ru/

REGISTRATION

The Agency is in charge of maintaining the Registry of Data Controllers.

Any data controller shall notify the Agency in writing about its intention to process personal data, unless one of the following exclusions applies:

- the personal data is exclusively data about employees;
- the personal data was received in connection with a contract entered into with the data subject, provided that such data is not transferred without the consent of the data subject, but used only for the performance of the contract and entering into contracts with the data subject (for example, data provided by a customer purchasing a product online and the data is used only to fulfil the order);
- the personal data is the data about members of a public or religious association and processed by such an organisation for lawful purposes in accordance with their charter documents, provided that such data is not transferred without the consent of the data subjects;
- the personal data was made publicly accessible data by the data subject;
- the personal data includes the surname, name and father's name only (Russia uses patronymic references in place of "middle" names);
- the personal data is necessary in order to give single access to the premises of the data controller or for other similar purposes;
- the personal data is included in state automated information systems or state information systems created for the protection of state security and public order;
- the personal data is processed in accordance with the law without any use of automatic devices; or
- the personal data is processed in accordance with transportation security legislation for the purposes of procurement of stable and secure transport complex and personal, community and state interests protection.

The notification letter shall contain information about:

- the full name and address of the data controller;
- the purpose of the processing;
- the categories of personal data processed;
- the categories of the subjects whose personal data is processed;
- the legal grounds for processing;
- the types of processing of the personal data;
- the measures of protection of personal data;
- name and contact information of the physical person or legal entity responsible for personal data processing;
- the commencement date;
- information on occurrence of cross border transfer of personal data;
- the term of processing or the conditions for termination of processing the personal data; and
- information on personal data security provision.

DATA PROTECTION OFFICERS

If the data controller is a legal entity, it is required to appoint a data protection officer. Such an appointment is considered to be a personal data protection measure. The data protection officer oversees compliance by the data controller and its employees

regarding the data protection issues, informs them of statutory requirements and organises the receiving and processing of communications from data subjects.

There are no legal restrictions as to whether the data protection officer should be a citizen or resident of the Russian Federation, however, it is adviseable that the data protection officer is available in case there is an inspection or other communication from the authorities.

Non-appointment or improper appointment of the data protection officer is a violation of the data protection regime and may result in the imposition of penalties and enforcement protocols, as described below.

COLLECTION & PROCESSING

Data controllers may collect and process personal data where any of the following conditions are met:

- the data subject consents;
- the processing is required by a federal law or under an international treaty;
- the processing is required for administration of justice, execution of a court order or any other statements of public officers to be executed;
- the processing is required for provision of state or municipal services;
- the data controller needs to process the data to perform or conclude a contract to which the data subject is a party or beneficiary party or guarantor;
- the processing is carried out for statistical or scientific purposes (except where processing is used also for advertising purposes) provided that it is impersonalised;
- the processing protects the data controller's vital interests and it is impossible to have the data subject's consent;
- the processing is required for execution of statutory controller's or third parties' rights or for purposes important for the community provided the data subject's rights are not in breach;
- personal data that is processed was publicly made accessible by the data subject or upon his or her request;
- the processing is carried out by a journalist or mass media as a part of its professional activities or for the purposes of scientific, literary or other creative activities, except if the processing would damage the data subject's rights and freedoms; or
- personal data that is processed is subject to publication or mandatory disclosure under law.

As a general rule, consents by a data subject may be given in any form, but it is the data controller's obligation to provide proof that he has the data subject's consent. Because of this burden of proof, it is important to keep careful records of consents.

In the following cases, the DPA requires that the data subject's consent should be in writing (preferably in hard copy form):

- where the personal data is collected to be included within publicly accessible sources;
- where sensitive or biometrical data is processed;
- in the case of the cross border transfer of personal data, where the recipient state does not provide adequate protection of personal data; or
- where a legally binding decision is made solely on the grounds of the automated processing of personal data.

Consent is deemed to have been given in writing where it is signed by hand or given in an electronic form and signed by an electronic signature.

Consent may be revoked.

Consent in writing must contain the following information:

- the identity of the data subject, his/her address and passport details and identity of the subject;
- data representative (if any);
- the identity and address of the data controller or the entity that processes personal data on behalf of the data controller (if any);
- the purpose of the processing;

- the list of personal data that may be collected and processed;
- the types of processing that are authorised;
- the term for which the consent, remains valid and way of revocation; and
- the data subject's signature.

The data controller shall ensure the confidentiality of personal data. The data controller and other persons who have access to the personal data, shall not disclose any information to a third party without the prior consent of the data subject.

TRANSFER

Prior to a transfer of personal data out of Russia, the data controller must ensure that the recipient state provides adequate protection of personal data. The fact that the recipient state ratified the Convention is sufficient grounds to deem that the state provides adequate protection of personal data for the purposes of the DPA.

Where there is no adequate protection of personal data, a cross border transfer is permitted if one of the following conditions is met:

- the data subject consents;
- the transfer is provided for under an international treaty to which Russia is a signatory;
- the transfer is necessary in accordance with federal laws for protection of the Constitution, state defence, security and transport system;
- for the purposes of performance of a contract to which the data subject is party; or
- the transfer protects the data subject's vital interests where it is not possible to get the written consent of the data subject.

In addition to the above, the *Roscomnadzor* issued the Order No. 274 of 15 March 2013 '*On endorsement of the List of the Foreign States Which are Not Parties to the EC Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data*'. The Order contains the list of countries which are officially recognized by Russian authorities as 'ensuring adequate protection'. Apart from the Member States of the Convention, there are 23 so 'white-listed' states as of today.

SECURITY

Data controllers are required to take appropriate technical and organisational measures against unauthorised or unlawful processing and accidental loss, changing, blocking or destruction of, or damage to, personal data.

A recent special regulation sets forth certain measures that the data controller should undertake to ensure security of personal data, data systems, carriers of biometrical information and technologies.

BREACH NOTIFICATION

There is no mandatory requirement to report data security breaches or losses to the Agency or to data subjects.

ENFORCEMENT

In Russia, the Agency is responsible for the enforcement of the DPA. The Agency is entitled to:

- carry out checks;
- consider complaints from data subjects;
- require the submission of necessary information about personal data processing by the data controller;
- require the undertaking of certain actions according to the law by the data processor, including discontinuance of the processing of personal data;
- file court actions;
- initiate criminal cases; and
- impose administrative liability.

If the Agency becomes aware that a data controller is in violation of the law, he can serve an enforcement notice requiring the

data controller to rectify the position.

A data controller can face civil, administrative or criminal liability if there is a violation of personal data law. Officers of the data controller responsible for the offence may also face disciplinary action.

Usually, in the case of violation of data protection law, the Agency will serve an enforcement notice requiring the position to be rectified and may also impose an administrative penalty and/or recommend imposing disciplinary action on the officers of the data controller who are responsible for the offence.

The maximum administrative penalty that can be imposed, as at the date of this review, is RUR (Russian Rubles) 75,000.

ELECTRONIC MARKETING

Electronic marketing activities are subject to limitations set by the Russian Law on Advertising No. 38-FZ dated 13 March 2006, under which the distribution of advertising through telecommunications networks, in particular, through the use of telephone, facsimile and mobile telephone communications, is allowed only subject to preliminary consent of a subscriber or addressee to receive advertising.

Advertising is presumed to be distributed without preliminary consent of the subscriber or addressee unless the advertising distributor can prove that such consent was obtained. The advertising distributor is obliged immediately to stop distribution of advertising to the address of the person who made such a demand.

ONLINE PRIVACY

Russian law does not specifically regulate online privacy. The definition of personal data under the DPA is rather broad and there are views that information on number, length of visits of particular web-sites and IP address (in combination with other data allowing the user to be identified) could be considered personal data.

KEY CONTACTS

Michael Malloy
Counsel and Head of Intellectual Property and Technology Practice
T +7 495 221 4400
michael.malloy@dlapiper.com

Pavel Arievich
Legal Director
T +7 495 221 4472
pavel.arievich@dlapiper.com

Ekaterina Golodinkina
Associate
T +7 495 221 4546
ekaterina.golodinkina@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SAUDI ARABIA

Last modified 25 January 2019

LAW

Shari'a principles (that is, Islamic principles derived from the Holy *Quran* and the *Sunnah*, the latter being the witnesses' sayings of the Prophet Mohammed), which although not codified, are the primary source of law in the Kingdom of Saudi Arabia (KSA). In addition to *Shari'a* principles, the law in the KSA consists of secular regulations passed by the government.

At this time, there is no specific data protection legislation in place in the KSA (although we understand that a new freedom of information and protection of private data law is under review by the formal advisory body of KSA, the Shura Council). *Shari'a* principles generally protect the privacy and personal data of individuals.

That said, there are certain secular regulations passed by government, which, although not dedicated as a whole to data privacy/protection, contain specific provisions governing the right to privacy and data protection in certain contexts.

There may also be specific regulations applicable to certain industries, for example, in banking, which is regulated by the Saudi Arabian Monetary Authority (SAMA).

DEFINITIONS

Definition of personal data

In the absence of specific data protection legislation, there is no definition of personal data.

Definition of sensitive personal data

In the absence of specific data protection legislation, there is no definition of sensitive personal data.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in the KSA.

REGISTRATION

In the absence of a national data protection authority, there are no data protection registration requirements in the KSA.

DATA PROTECTION OFFICERS

There is no requirement in the KSA for organizations to appoint a data protection officer.

COLLECTION & PROCESSING

There is no concept of data controller or data processor in the KSA.

TRANSFER

There is no specific data protection legislation in place in the KSA.

In certain contexts or sectors, specific approvals may be required—for example, in a banking context, approval from SAMA.

SECURITY

There is currently no dedicated date protection legislation imposing specific security requirements.

BREACH NOTIFICATION

There are no dedicated data protection regulations imposing a mandatory requirement to report data security breaches.

ENFORCEMENT

At this time, there is no clear designated authority responsible for the enforcement of data protection and privacy equivalent to, say, the Information Commissioner in the United Kingdom. That said, specific authorities are tasked with enforcing breaches of other legislation that is in place in the KSA.

ELECTRONIC MARKETING

Electronic marketing is regulated by the Communications and Information Technology Commission, and is subject to various requirements. Generally, it is advisable to obtain prior consent before sending electronic marketing messages to individuals in KSA.

ONLINE PRIVACY

There is no specific legislation in the KSA that expressly regulates the use of cookies.

KEY CONTACTS

Mohamed Moussallati
Senior Legal Consultant
T +966 11 201 8900
mohamed.moussallati@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SERBIA

Last modified 28 January 2019

LAW

In late 2018, Serbia updated its data protection law to better align with the EU General Data Protection Regulation. Serbia enacted a new Data Protection Law on November 9, 2018 (published in the Official Gazette of the Republic of Serbia, no. 87/2018) (New DP Law). The New DP Law entered into force November 21, 2018, but its effective date has been postponed until August 21, 2019 (except for the maintenance of the Central Register of Personal Databases which has already been terminated). The New DP Law was long awaited, as it has been 10 years since the existing law was passed. Its content is largely harmonized with the GDPR.

Until the New DP Law becomes fully applicable on August 21, 2019, the Serbian law governing data protection issues remains the Law on Protection of Personal Data (Official Gazette of the Republic of Serbia, nos. 97/2008, 104/2009, 68/2012 and 107/2012) (DP Law). It became applicable on January 1, 2009, and its current version (incorporating supplements made in 2012) is in force as of November 17, 2012.

DEFINITIONS

Definition of personal data

Under the DP Law and the New DP Law, personal data is any information about a natural person through which the respective person is identified or identifiable (for example, name, address, email address, photo, etc.).

NATIONAL DATA PROTECTION AUTHORITY

The Serbian data protection authority is the Commissioner for Information of Public Importance and Protection of Personal Data (*Poverenik za informacije od javnog znaaja i zaštitu podataka o linosti*) (DPA).

It is seated at Bulevar kralja Aleksandra 15 Belgrade and its website is www.poverenik.rs.

REGISTRATION

The only exception to the New DP Law's postponed implementation is the obligation of the maintenance of the Central Register of Personal Databases by the DPA, which is terminated immediately upon the entering into force of the New DP Law. Notwithstanding the above, the transitional provisions of the New DP Law did not formally terminate the existing obligation for the companies to file the database notifications (probably due to a technical omission), and therefore formally this obligation still applies until August 21, 2019. Under the New DP Law, controllers and processors will only be required to internally maintain the database records and, in certain cases, even that obligation will not apply to companies with up to 250 employees.

Under the DP Law, any person or legal entity that processes personal data in Serbia (and, based on the relevant processing, establishes a database containing personal data) has to report the relevant processing to the DPA.

This database reporting obligation generally consists of two phases. The first phase is to notify the DPA of the intention to

establish a database (at the latest 15 days prior to the intended database establishment date). The second phase is to report to the DPA that the respective database was created (at the latest 15 days from the date of its creation). Both phases are performed by filing prescribed forms with the DPA; the respective forms contain specific data on the data controller (such as its name and address of its registered seat) and on the database itself (for example, the purpose of and legal ground for its establishment, identification of exact processing activities, types of processed data, categories of data subjects, etc.). Any subsequent change to the reported database (for example, change of the initially reported processing activities) has to be reported to the DPA as well, at the latest 15 days from the date when the particular change occurred.

DATA PROTECTION OFFICERS

According to the DP Law, there is no statutory obligation for an entity which processes personal data to have a data protection officer (DPO).

However, according to the New DP Law, controllers and processors will be required to designate the DPO, whose primary tasks will be to ensure compliance with the data processing law and regulations and to communicate with the DPA and the data subjects on all data protection matters. Similar to the GDPR, this obligation applies if the following criteria are met:

- The processing is carried out by a public authority (with the exception of a court performing its judiciary authorizations).
- The core activities of the controller/processor require the regular and systematic monitoring of data subjects on a large scale, or the large-scale processing of special categories of personal *data—eg,* health data or trade union memberships, or criminal convictions / offenses data.

The DPO may be employed or engaged under a service contract, and in any case must have sufficient expert knowledge. A group of companies may appoint a single DPO, provided that he is equally accessible by each company.

Controllers and processors are required to ensure the DPO's independence in the performance of his tasks. This means the following:

- No instructions may be given to the DPO.
- The DPO must report directly to the manager of the controller / processor.
- The DPO may not be dismissed or penalized for performing his or her tasks.

COLLECTION & PROCESSING

The collection and further processing of personal data has to be legitimate and legally grounded, meaning pursuant to the data subject's consent or as specifically provided by law.

Under the DP Law and the New DP Law, there are a few cases when a data subject's personal data may be processed without the data subject's consent (for example, when the processing is necessary for fulfilment of the data controller's statutory obligations or for preparation or realization of an agreement concluded between a data controller and data subject) (Exceptional Cases).

Apart from the Exceptional Cases, prior, informed consent from data subjects is generally required to collect and process personal data, meaning that it has to contain all the information on the particular processing which is explicitly prescribed by the DP Law and the New DP Law (for example, the data subject must be notified of the purpose of the processing, identification of exact processing activities, information on other users of the data in cases when the data controller is not its only user, information on statutory rights of the data subjects in relation to the respective processing, etc.)

Although consent is necessary, it does not automatically mean that any processing, to which a data subject has consented, will be regarded by the DPA as compliant with the DP Law and the New DP Law. There are also other conditions which must be met under the DP Law and the New DP Law (*eg*, the purpose must be legitimate and clearly determined and the type and scope of processed data must be proportionate to the respective purpose).

As opposed to the existing law, which recognizes only hand-signed consent in the written form — creating significant issues in the digital age — the New DP Law explicitly introduces other forms as well, such as online and oral consent, or consent by other clear affirmative action, provided that the controller is able to demonstrate that the data subject has indeed consented.

On the other hand, the conditions for obtaining consent have become much stricter under the New DP Law: similar to the GDPR, consent must be freely given, specific, informed and unambiguous. For example, there is a presumption that consent will not be valid unless separate consents are obtained for different processing operations, where appropriate; and the request for consent—when presented in a written document—must be clearly distinguishable from all other matters, using clear and plain language (meaning catch-all clauses will not be valid. Further, consent will not be considered freely given if the performance of a contract is conditional on the consent to the processing of personal data that is not necessary for its performance.

In addition, one among many important novelties introduced by the New DP Law (and similar to the GDPR), is that it will not apply only to the processing of data carried out by Serbian controllers and processors, but will also apply to the processing of data by controllers and processors based outside of Serbia whose processing activities relate to the offering of goods or services (even if offered for free) or monitoring the behavior of Serbian data subjects within Serbia. As a result, a number of these controllers and processors will need to appoint their representatives in Serbia, to be addressed by the DPA and the data subjects on all issues related to processing.

TRANSFER

The rules on the transfer of personal data, as envisaged by the DP Law, are quite general. Under the respective rules, there are two regimes for data transfer out of Serbia depending on whether the transfer will take place with or without the DPA's prior approval. The determining factor is whether a country to which the data is to be transferred is a member state of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Relevant Convention"). If a country to which the data is to be transferred has signed and ratified the Relevant Convention (such as, for example, the EU countries), the transfer from Serbia is free in the sense that it is not conditional upon prior data transfer approval of the DPA ("Transfer Approval"), otherwise, Transfer Approval is necessary (such as, for example, for a transfer to the US).

However, according to the New DP Law, the data transfer regime has been completely revamped and liberalized, which is a much-welcomed change from the current overly restrictive concept. The New DP Law explicitly applies to both direct and indirect data transfers, unlike the existing law for which it is not fully clear whether it covers indirect transfers at all.

Under the New DP Law, controllers will be entitled to transfer personal data abroad if one of the following conditions (among others) is met:

- Personal data is to be transferred to a country that ratified the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data.
- Data transfers are performed to a country included on the EU list or the Serbian government's list of countries providing an adequate level of data protection.
- Data transfers are performed to a country which has a bilateral agreement with Serbia regulating data transfers.
- The transfer is based on the standard contractual clauses prepared by the Serbian DPA.
- The transfer is based on binding corporate rules or a code of conduct approved by the Serbian DPA, or on certificates issued in accordance with the new law.
- The Serbian DPA has issued a specific approval for the transfer to be performed on the basis of an agreement between the data exporter and the data importer.
- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks.

This should create more options for the transfer of data to non-European countries, especially once the DPA prepares the standard contractual clauses, which should be based on those approved by the EU Commission. In addition, it is expected that the process of obtaining the DPA's approval for such transfers will be more efficient, and should be completed within 60 days (currently the procedure often lasts for more than one year).

SECURITY

There are no specific security measures prescribed by the DP Law. It is only generally prescribed that:

- Personal data must be adequately protected from abuse, destruction, loss, unauthorized alterations or access
- Both data controllers and processors are to undertake all necessary technical, human resources and organizational measures to protect data from loss, damage, inadmissible access, modification, publication and any other abuse, as well as

to provide for an obligation of keeping data confidentiality for all persons who work on data processing

Similar to the GDPR, the New DP Law introduces burdensome accountability obligations on data controllers, which are required to "demonstrate compliance." This includes their obligation to all of the following:

- Implement, maintain and update appropriate technical and organizational measures to ensure a level of security appropriate to the risk-taking into account the state of the art, the associated implementation costs etc.
- Have in place certain documentation, such as data protection policies and records of processing activities
- Implement data protection by design and by default
- Conduct a data protection impact assessment for those processing operations that are considered more of risk to the rights and freedoms of individuals

Data protection by design requires the controllers to adopt, as well as maintain and update when needed, appropriate measures—such as pseudonymization, data minimization—which will integrate the safeguards necessary for processing. Data protection by default, on the other hand, requires the controllers to adopt measures so that, by default, only the processing which is necessary for the specific purpose will be possible (*eg*, that, by default, privacy settings on one's social network profile do not make his data public).

BREACH NOTIFICATION

While the DP Law does not impose a duty to notify a data security breach, as explained below, the New DP Law imposes data breach notification obligations that largely track the GDPR. Further, the Law on Electronic Communications ('Official Gazette of the Republic of Serbia', nos. 44/2010, 60/2013, 62/2014 and 95/2018) (EC Law) imposes a duty on entities which perform or are authorized to perform electronic communications' activities (Operators) to notify the Regulatory Agency for Electronic Communications and Postal Services (RATEL) as the competent state authority, of any breach of security and integrity of public communication networks and services, which has influenced their work significantly, and particularly on the breaches which resulted in violation of protection of personal data or privacy of the respective networks/services' users / subscribers.

Nonperformance of this statutory obligation can lead to liability and fines ranging from €4,250 to €16,950 for a legal entity, and in range from €425 to €1,270 for a responsible person in a legal entity. Protective measures may also be implemented: for a legal entity, a prohibition against performing business activities for a duration of up to three years, and, for a responsible person in a legal entity, a prohibition against performing certain duties for a duration of up to one year. According to the New DP Law, the data breach obligations present a significant novelty, as data controllers will generally be required to document each data breach—as well as to notify the DPA of most of them—without undue delay and, when feasible, within 72 hours after becoming aware of the breach. In addition, data processors will have to notify the controllers of the breach without undue delay.

If the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller is also required to communicate the personal data breach to the concerned individual as well, without undue delay. However, this does not apply if the controller has implemented appropriate technical and organizational measures, such as encryption that has rendered the relevant data unintelligible to any unauthorized person; or, if the notification would involve disproportionate efforts, a public communication or a similar measure must be made in order to properly inform the individuals.

ENFORCEMENT

The DPA is responsible for the enforcement of the DP Law and the New DP Law. Namely, the DPA is authorized and obliged to monitor whether the law is implemented and it conducts such monitoring both ex officio and based on any complaints it receives. If it establishes, when performing the respective monitoring, that a particular person / entity which processes personal data has acted in contravention to the statutory rules on processing, the DPA shall issue a warning to the particular data controller. It may also issue a decision by which it can, among other things:

- Order the data controller to eliminate the existing irregularities within a certain period of time
- Temporarily forbid particular processing
- Order deletion of the data collected without a legal ground

The DPA's decision cannot be appealed, but an administrative dispute can be initiated against the respective decision before a

competent Serbian court.

Depending on the gravity of the particular misconduct and the data controller's behavior with respect to the same, the DPA can initiate an offense proceeding against the respective data controller before the competent court. The offenses and sanctions for such are explicitly prescribed by the DP Law. The respective sanctions are fines (ranging from €425 to €8,480 for a legal entity and from €42 to €425 for a responsible person in a legal entity). According to the New DP Law, the respective sanctions are fines up to €16,950 for a legal entity and up to €1,270 for a responsible person in a legal entity. Additionally, the DPA is now also able to fine the controllers and processors directly in certain situations, with fines in the amount of €850. Until the adoption of the New DP Law, only the Court of Offences was entitled to impose fines.

Criminal liability is also a possibility since the Serbian Criminal Code prescribes a criminal offense of unauthorized collection of personal data. The prescribed sanctions are a monetary fine (of an amount to be determined by the court) or imprisonment of up to one year. Both natural persons and legal entities can be subject to the respective liability.

Formally speaking, under the Law on Administrative Procedure ('Official Gazette of the Republic of Serbia', nos. 18/2016 and 95/2018), the DPA is also authorized to enforce its orders by threatening a company with a fine of up to 10% of its annual income in Serbia, in case it fails to comply with the order. This is a relatively new option for Serbian authorities that has not yet been tested in practice, to the best of our knowledge.

ELECTRONIC MARKETING

Electronic marketing is not governed by the DP Law, while in the New DP Law is only mentioned in the context of data subjects' complaint right. The rules on this subject are envisaged by the Law on Electronic Trade ('Official Gazette of the Republic of Serbia', nos. 41/2009 and 95/2013), EC Law (as defined above in the section on Breach Notification), the Law on Advertising ('Official Gazette of the Republic of Serbia', no. 6/2016) and the Consumer Protection Law (Official Gazette of the Republic of Serbia, nos. 62/2014, 6/2016 and 44/2018) (together, the "Relevant Legislation").

In brief, based on the Relevant Legislation, electronic marketing is only allowed if it is covered by an explicit, prior written consent of the person to whom the respective marketing is directed. Additionally, recipients should always be:

- Clearly informed of the identity of the sender and commercial character of the communication (this information should be provided in the Serbian language prior to commencing the marketing)
- Provided with a way to opt out of future marketing messages, at any time and free of charge

ONLINE PRIVACY

There are no specific regulations explicitly governing online privacy (including cookies). Accordingly, the general data protection rules, as introduced by the DP Law and the New DP Law, are, to the extent applicable, relevant for online privacy as well.

On the other hand, it should be noted that the EC Law, as defined in the section on Breach Notification above, introduces rules on the processing of traffic data and location data, which are obligatory for entities which are the Operators (as defined above in the section on Breach Notification) of public communication networks and publicly available electronic communication services. Under these rules, these Operators are allowed to do the following:

- Process traffic data only as long as such data is necessary for a communication's transmission and thus, when such necessity ceases to exist, the Operators are obliged, unless exceptionally (for example, in the case when they have obtained prior consent of the data subjects for using the respective data for marketing purposes), to delete such data or to keep them but only if they make the persons to which the date relates unrecognizable
- Process location data generally only if the persons to which the data relates are made unrecognizable or if they have such persons' prior consent for the purpose of providing them with value added services (but even if such consent does exist, only in the scope and for the time during which the processing is needed for the respective purpose's realization)

Violations are subject to the fines set forth above in the Breach Notification section.

KEY CONTACTS

Karanovic & Nikolic
www.karanovic-nikolic.com/

Sanja Spasenovic
Attorney at law in cooperation with Karanovic & Partners
Karanovic & Partners
T Office +381 11 3094 200/ Direct T +381 11 3955 413
Sanja.Spasenovic@karanovicpartners.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SEYCHELLES

Last modified 25 January 2017

LAW

The Data Protection Act (the 'Act') was enacted in 2003 (Act No. 9 of 2003) with the aim of protecting the fundamental privacy rights of individuals against the use of data concerning them without their informed consent. The Act will come into operation on such date as the Minister notifies in the official Gazette.

As of May 2015, the Act has not yet come into operation.

DEFINITIONS

Definition of personal data

Personal data is defined under the Act as data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user), including any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual.

Definition of sensitive personal data

The Act does not define sensitive personal data. However the Act makes provision for the Minister to modify or supplement the Data Protection Principles set out in the Act for the purpose of providing additional safeguards in relation to personal data consisting of information as to:

- the racial origin of the data subject
- his political opinions or religious or other beliefs
- his physical or mental health or his sexual life, or
- his criminal convictions.

NATIONAL DATA PROTECTION AUTHORITY

The creation of the Office of the Data Protection Commissioner is envisaged by the Act but has not yet taken place.

REGISTRATION

A person shall not hold personal data unless an entry in respect of that person as a data user, or as a data user who also carries on a computer bureau, is for the time being contained in the register of data users maintained by the Data Protection Commissioner.

The particulars to be entered into the data register are as follows:

- the name and address of the data user

- a description of the personal data to be held by it and of the purpose or purposes for which the data is to be held or used
- a description of every source from which it intends or may wish to obtain the data or the information to be contained in the data
- a description of every person to whom it intends or may wish to disclose the data (otherwise than in cases of exemptions from non-disclosure as set out in the Act)
- the name of every country outside Seychelles to which it intends or may wish directly or indirectly to transfer the data, and
- one or more addresses for the receipt of requests from data subjects for access to the data.

A person applying for registration shall state whether he wishes to be registered as a data user, as a person carrying on a computer bureau or as a data user who also carries on a computer bureau, and shall furnish the Data Protection Commissioner with the particulars required to be included in the entry to be made in pursuance of the application. Where a person intends to hold personal data for two or more purposes he may make separate applications for registration in respect of any of those purposes.

A registered person may at any time apply to the Data Protection Commissioner for the alteration of any entries relating to that person. Where the alteration would consist of the addition of a purpose for which personal data are to be held, the person may make a fresh application for registration in respect of the additional purpose.

The Data Protection Commissioner shall, as soon as practicable and in any case within the period of 6 months after receiving an application for registration or for the alteration of registered particulars, notify the applicant in writing whether his application has been accepted or refused. Where the Commissioner notifies an applicant that his application has been accepted, the notification must state the particulars which are to be entered in the register, or the alteration which is to be made, as well as the date on which the particulars were entered or the alteration was made.

No entry shall be retained in the register after the expiration of the initial period of registration except in pursuance of a renewal application made to the Data Protection Commissioner. The initial period of registration and the period for which an entry is to be retained in pursuance of a renewal application ('the renewal period') shall be a period 5 years beginning with the date on which the entry in question was made or, as the case may be, the date on which that entry would fall to be removed if the application had not been made.

The person making an application for registration or a renewal application may in his application specify as the initial period of registration or, as the case may be, as the renewal period, a period shorter than five years, being a period consisting of one or more complete years.

DATA PROTECTION OFFICERS

The Act does not contain any legal requirement to appoint a data protection officer.

COLLECTION & PROCESSING

The data protection principles set out in the Act apply to personal data held by data users. Those data protection principles are as follows:

- the information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully
- personal data shall be held only for one or more specified and lawful purposes
- personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes
- personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose

or those purposes

- personal data shall be accurate and, where necessary, kept up to date
- personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
- an individual shall be entitled:
    - at reasonable intervals, and without undue delay or expenses to be informed by any data user whether he holds personal data of which that individual is the subject
    - to access to any such data held by a data user, and
    - where appropriate, to have such data corrected or erased.

TRANSFER

If it appears to the Data Protection Commissioner that a person registered as a data user (or as a data user who also carries on a computer bureau) intends to transfer personal data held by him to a place outside the Seychelles, the Data Protection Commissioner may, if satisfied that the transfer is likely to contravene or lead to a contravention of any data protection principle, serve that person with a transfer prohibition notice prohibiting him from transferring the data either absolutely or until he has taken such steps as are specified in the notice for protecting the interests of the data subjects in question.

In deciding whether to serve a transfer prohibition notice, the Data Protection Commissioner shall consider whether the notice is required for preventing damage or distress to any person and shall have regard to the general desirability of facilitating the free transfer of data between the Seychelles and other states.

A transfer prohibition notice shall specify the time when it is to take effect and contain a statement of the principle or principles which the Data Protection Commissioner is satisfied are contravened and his reasons for reaching that conclusion, as well as particulars of the right of appeal conferred by the Act.

The Data Protection Commissioner may cancel a transfer prohibition notice by written notification to the person on whom it was served.

No transfer prohibition notice shall prohibit the transfer of any data where the transfer of the information constituting the data is required or authorised by or under any enactment or is required by any convention or other instrument imposing an international obligation on the Seychelles.

Any person who contravenes a transfer prohibition notice shall be guilty of an offence but it shall be a defence for a person charged with an offence under this subsection to prove that he exercised all due diligence to avoid a contravention of the notice in question.

SECURITY

The Act provides that appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

BREACH NOTIFICATION

Breach notification

There is no mandatory requirement in the Act to report data security breaches or losses to the Data Protection Commissioner. However, the Act provides that the Data Protection Commissioner may consider any complaint that any of the data protection principles or any provision of this Act has been or is being contravened and shall do so if the complaint appears to him to raise a matter of substance and to have been made without undue delay by a person directly affected.

Where the Data Protection Commissioner investigates any such complaint he shall notify the complainant of the result of his investigation and of any action which he proposes to take.

Mandatory breach notification

None contained in the Act.

ENFORCEMENT

If the Data Protection Commissioner is satisfied that a registered person has contravened or is contravening any of the data protection principles, the Data Protection Commissioner may serve that person with an enforcement notice requiring him to take such steps for complying with the principle or principles in question. In deciding whether to serve an enforcement notice the Data Protection Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress.

An enforcement notice in respect of a contravention of the data protection principle concerning data accuracy may require the user to rectify or erase the data and any other data held by him containing an expression of opinion which appears to the Data Protection Commissioner to be based on the inaccurate data.

If by reason of special circumstances the Data Protection Commissioner considers that the steps required by an enforcement notice should be taken as a matter of urgency, he may include a statement to that effect in the notice.

The Data Protection Commissioner may cancel an enforcement notice by written notification to the person on whom it was served.

Any person who fails to comply with an enforcement notice shall be guilty of an offences; but it shall be a defence for the person charged with an offence under this subsection to prove that he exercised all due diligence to comply with the notice in question.

If the Data Protection Commissioner is satisfied that a registered person has contravened or is contravening any of the data protection principles, the Commissioner may serve the person with a de-registration notice stating that the Data Protection Commissioner proposes to remove from the register all or any of the particulars constituting the entry or any of the entries contained in the register in respect of that person. In deciding whether to serve a de-registration notice, the Data Protection Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress, and the Data Protection Commissioner shall not serve such a notice unless he is satisfied that compliance with the principle or principles in question cannot be adequately secured by the service of an enforcement notice.

ELECTRONIC MARKETING

Although not specifically provided for in the Act, the latter will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (for instance, an email is likely to be considered as personal data for the purposes of the Act).

ONLINE PRIVACY

The Act does not contain specific provisions in relation to online privacy.

KEY CONTACTS

Juristconsult Chambers
www.juristconsult.com

Shalinee Dreepaul Halkhoree
Partner-Barrister
T +230 465 00 20 Extension 225
sdreepaul@juristconsult.com

Arvin Halkhoree
Barrister
T +(230) 208 5526
ahalkhoree@juristconsult.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SINGAPORE

Last modified 28 January 2019

LAW

Singapore enacted the Personal Data Protection Act of 2012 (No. 26 of 2012) (the Act) on October 15, 2012. The Act took effect in three phases:

1. Provisions relating to the formation of the Personal Data Protection Commission (the Commission) took effect on January 2, 2013.
2. Provisions relating to the National Do-Not-Call Registry took effect on January 2, 2014.
3. The main data protection provisions took effect on July 2, 2014.

The Act has extraterritorial effect, meaning it applies to organizations collecting personal data from individuals in Singapore whether or not the organization itself has a physical presence in Singapore.

The data protection obligations under the Act do not apply to the public sector, to whom separate rules apply.

The Commission's first public consultation reviewing the Act (PDPA Consultation) closed in October 2017, and focused on "approaches to managing personal data in the digital economy," with topics including "challenges for alternatives to consent" and mandatory breach notification. It is anticipated that the Act will be amended sometime in 2019 to incorporate the changes proposed in the PDPA Consultation.

DEFINITIONS

Definition of personal data

Personal data is defined in the Act to mean data, whether true or not, about an individual (whether living or recently deceased*) who can be identified:

- From that data; or
- From that data and other information to which the organization has, or is likely to have access

*The Act's application to recently deceased individuals is limited to disclosure and protection of personal data where such data is about an individual who has been deceased for ten years or fewer.

The data protection obligations under the Act do not apply to business contact information. This excludes from the Act the following if provided solely for business purposes:

- Name
- Position name or title
- Business telephone number
- Business address

- Business electronic mail address
- Business fax number

It is important to note that the Act still governs business contact information provided by individuals solely in their personal capacity. Where the purposes of provision of business contact information are mixed (that is, for both business and personal purposes), the Act does not apply.

Definition of sensitive personal data

There is no definition of sensitive personal data in the Act.

However, non-binding guidance from the Commission indicates that sensitivity of data is a factor for consideration in implementing policies and procedures to ensure appropriate levels of security for personal data. For example, encryption is recommended for sensitive data stored in an electronic medium that has a higher risk of adversely affecting the individual should it be compromised. Where any personal data collected is particularly sensitive (*eg*, regarding physical or mental health), as a matter of best practice, such data should only be used for limited purposes and the security measures afforded to such data should take into account the sensitivity of the data.

The Commission has also stated in its enforcement decisions that the fact that personal data is of a sensitive financial nature is a relevant factor in its decisions, and a public condition in 2017 proposed draft additional safeguards for collection, use and disclosure of National Identification Registration Card (NRIC) numbers.

NATIONAL DATA PROTECTION AUTHORITY

Personal Data Protection Commission

460 Alexandra Road
#10-02 PSA Building
Singapore 119963

T +65 6377 3131
F +65 6273 7370

info@pdpc.gov.sg
http://www.pdpc.gov.sg/

REGISTRATION

There are no registration requirements under the Act.

While not a requirement, in April 2017 the Commission publicly encouraged organizations to register their Data Protection Officers (DPOs) with the Commission via the Commission's website, to assist DPOs in keeping up to date with developments in the law.

DATA PROTECTION OFFICERS

Each organization must appoint one or more data protection officers to be responsible for ensuring the organization's compliance with the Act. An organization may appoint one person or a team of persons to be its DPO. Once appointed, the DPO may in turn delegate certain responsibilities, including to non-employees of the organization. The business contact information of the DPO must be made available to the public.

While there is no requirement for the data protection officer to be a citizen or resident in Singapore, the Commission suggests that the data protection officer should be readily contactable from Singapore, available during Singapore business hours and, where telephone numbers are provided, these should be Singapore telephone numbers.

Failure to appoint a data protection officer may lead to a preliminary investigation by the Commission. If an organization or an

individual fails to cooperate with the investigation, this will constitute an offense. As a result, an individual may be subject to a fine of up to S$10,000 or imprisonment for a term not exceeding 12 months, or to both. An organization may be subject to a fine of up to S$100,000.

COLLECTION & PROCESSING

Organizations may only collect, use or disclose personal data in the following scenarios:

- They obtain express consent from the individual prior to the collection, use, or disclosure of the personal data (and such consent must not be a condition of providing a product or service, beyond what is reasonable to provide such product or service; and must not be obtained through the provision of false or misleading information or through deceptive or misleading practices), and have also provided the relevant data protection notice (notifying purposes of collection, use and disclosure) to the individual before, or at the time when they are collecting, using or disclosing the personal data
- There is deemed consent by the individual to the collection, use, or disclosure of the personal data in accordance with the relevant conditions of the Act
- Where the limited specific exclusions prescribed in the Act apply (if no consent or deemed consent is given)

An individual may at any time withdraw any consent given, or deemed given under the Act, upon giving reasonable notice to the organization.

Further, any collection, use or disclosure of the personal data must only be for the purposes that a reasonable person would consider appropriate in the circumstances, and for purposes to which the individual has been notified of. Such notification must be made in accordance with the requirements of the Act.

An organization must also do all of the following:

- Make information about its data protection policies, practices and complaints process publicly available
- Cease to retain personal data or anonymize it where it is no longer necessary for any business or legal purpose
- Ensure personal data collected is accurate and complete if likely to be used to make a decision about the individual or disclosed

New data protection management program (DPMP) and data protection impact assessment (DPIA) guides were published by the Commission in November 2017.

In addition, due to the sensitive nature of the information contained in the National Identification Registration Card (NRIC) (and other similar forms of identification) and the physical card, new guidelines were published in August 2018 to provide organizations with guidance on the collection of the information contained in the NRIC as well as the collection of the physical card. From September 1, 2019, organizations will not be permitted to collect the NRIC or other national identification numbers or the physical cards, unless required by law, or if the collection is necessary for the verification of an individual's identity to high fidelity.

TRANSFER

In disclosing or transferring personal data to onshore third parties (including affiliates), an organization should ensure that it has obtained the individual's deemed or express consent to such transfer (unless exemptions apply) and, if this was not done at the time the data was collected, additional consent will be required (unless exemptions apply).

The Act also contains offshore transfer restrictions, which require an organization to ensure "comparable protection" to the standards set out in the Act when transferring personal data outside of Singapore. Mechanisms to achieve this include (this is not a comprehensive list): data transfer agreements (for which the Commission has recently released guidance, including model clauses); the individual has given consent (and provided required notices have been provided); and where transfers are considered necessary in certain prescribed circumstances (which include in connection with performance of contracts between the transferring organization and the individual, subject to certain conditions being met). An organization may apply to be exempted from any requirement prescribed under the Act in respect of any transfer of personal data out of Singapore. An exemption may be granted on such conditions as the Commission may require.

The Commission has published a new guide to data sharing (covering intragroup and third party sharing) with practical nonbinding guidance for organizations, as well as DPMP and DPIA guides (see Collection & Processing).

SECURITY

Organizations must protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks. The Act does not specify security measures to adopt and implement, however the Commission has issued best practice guidance which provides specific examples, including with respect to cloud computing and IT outsourcing.

BREACH NOTIFICATION

Currently, there are no mandatory requirements under the Act for data users to notify the Commission or individuals regarding data protection breaches in Singapore. The Commission issued a best practice guide in May 2015 to help organizations manage personal data breaches effectively, and more recent guidelines provide practical tips on avoiding and managing risks such as accidental data disclosure. It is recommended that affected individuals be notified immediately if a data breach involves sensitive personal data. The Commission should be notified as soon as possible of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals. Aggrieved parties may either make a complaint to the Commission, or may take out a private action in civil proceedings. The Commission may also conduct investigations on its own motion.

However, there are now proposals to introduce mandatory data breach notifications in Singapore. It is anticipated that the Act will be amended sometime in 2019 to incorporate the amendments proposed in the PDPA Consultation. Organizations are advised to monitor developments.

In addition, the Cybersecurity Act 2018 (CSA) was recently passed in Parliament, and sections of the CSA have now come into force. As at the date of this update, the obligations under the CSA primarily fall on organizations which have been designated as owners of critical information infrastructure. If your organization has been designated by the Cybersecurity Commissioner as the owner of a critical information infrastructure, additional obligations will apply to your organization in relation to data breach incident handling and notification.

ENFORCEMENT

Enforcement of the Act is carried out by the Commission. The powers of the Commission include giving directions to do any of the following:

- Stop collection, use or disclosure of personal data in contravention of the Act
- Destroy personal data collected in contravention of the Act
- Provide or refuse access to or correction of personal data
- Pay a financial penalty not exceeding S$1 million

These directions may be registered with the Singapore District Courts so that they may have the force and effect of an order of court.

The Commission published the *Advisory Guidelines on Enforcement of Data Protection Provisions* in April 2016. These guidelines indicate how in practice the Commission proposes to handle complaints, reviews and investigations of breaches of the data protection rules under the Act, and to approach enforcement and sanctions. Amongst other things, they set out the Commission's enforcement objectives, and guidance regarding the mitigating and aggravating factors that the Commission will take into account when issuing directions and sanctions (for example, prompt initial response and resolution of incidents; cooperation with investigations; and breach notification). The Commission has in the past couple of years stepped up its efforts to enforce the Act, highlighting the growing risks of non-compliance with the Act in Singapore.

Directions or decisions given are subject to reconsideration by the Commission, upon written application by any aggrieved party.

Directions, decisions or reconsiderations of the Commission may also be subject to appeal to a Data Protection Appeal Committee, unless the direction or decision to be appealed is the subject of an application for reconsideration, in which case such

appeal would be deemed withdrawn.

Directions may only be appealed to the High Court and Court of Appeal with regard to the following:

- A point of law arising from a direction or decision of the Appeal Committee
- Any direction of the Appeal Committee as to the amount of a financial penalty

Any person who has suffered loss or damage directly as a result of a contravention of the Act is also entitled to pursue a private action in court. However, where the Commission has made a decision with regard to the said loss or damage, a right of private action will only lie after the decision has become final as a result of there being no further right of appeal. The court may grant to the plaintiff all or any of the following:

- Relief by way of injunction or declaration
- Damages
- Such other relief as the court thinks fit

ELECTRONIC MARKETING

The data protection principles in the Act apply to any marketing activities (including electronic marketing) which involve the collection, use or disclosure of personal data.

In addition, any organization or person that wishes to engage in any telemarketing activities will need to comply with the "Do Not Call" provisions under the Act. Generally, a person or organization who wishes to send marketing messages to a Singapore telephone number should first obtain the clear and unambiguous consent of the individual to the sending of the messages to such Singapore telephone number. The consent must be evidenced in written or other form so as to be accessible for subsequent reference; must not be a condition for supplying goods, services, land, interest or opportunity; and must not be obtained through the provision of false or misleading information or through deceptive or misleading practices. In the absence of such consent, organizations must check and ensure that the telephone number is not on a Do-Not-Call register maintained by the Commission (DNC Register), unless such checks are exempted under the Act. There are also other requirements, including a duty to identify the sender of the marketing message and provide clear and accurate contact information, as well as a duty not to conceal the calling line identity of any voice calls containing such marketing message. An individual may at any time apply to the Commission to add or remove his Singapore telephone number on the DNC Register.

The Act will apply to marketing messages addressed to a Singapore telephone number in the following circumstances:

- The sender of the marketing message is present in Singapore when the message was sent.
- The recipient of the marketing message is present in Singapore when the message is accessed.

Electronic marketing activities are also regulated under the Spam Control Act (Cap 311A) (SCA), to the extent that such activities involve the sending of unsolicited commercial communications in bulk by electronic mail or by SMS or MMS to a mobile telephone number.

The Commission had a public consultation in April 2018 seeking views on the streamlining of the requirements under the "Do Not Call" provisions of the Act with the provisions under the SCA. The public consultation closed in June 2018, and organizations are advised to monitor developments in this area.

ONLINE PRIVACY

Currently, there are no specific requirements relating to online privacy (including cookies and location) under the Act. Nevertheless, an organization that wishes to engage in any online activity that involves the collection, use or disclosure of personal data will still need to comply with the general data protection obligations under the Act. For example, if an organization intends to use cookies to collect personal data, it must obtain consent before use of any such cookies. For details of the consent required, please see the Collection & Processing chapter. The Commission has published nonbinding guidelines providing practical tips on pertinent topics such as securing electronic personal data and building websites, and a public consultation as "approaches to managing personal data in the digital economy" was undertaken by the Commission in Summer 2017.

KEY CONTACTS

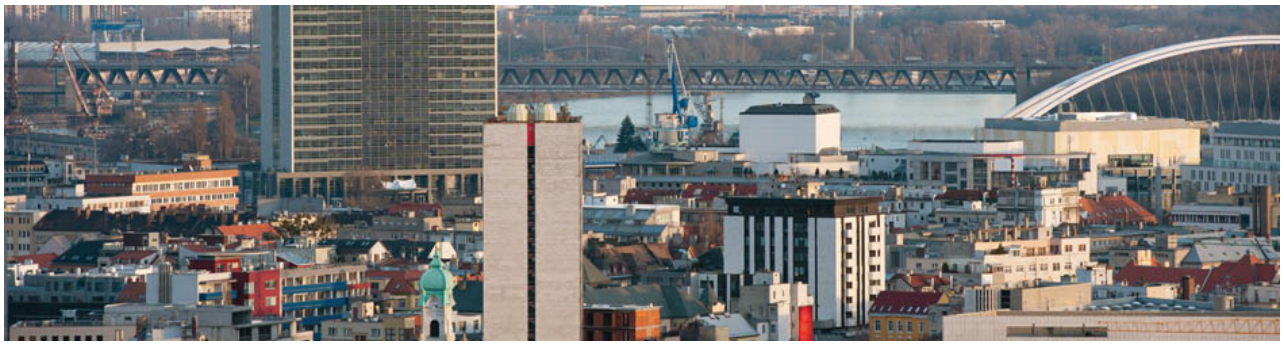
Scott Thiel
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +852 2103 0519
scott.thiel@dlapiper.com

Carolyn Bigg
Of Counsel
T +852 2103 0576
carolyn.bigg@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SLOVAK REPUBLIC



Last modified 14 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

As a member of the European Union, Slovakia is bound by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (the "**GDPR** ").

Furthermore, Slovakia adopted Act No. 18/2018 Coll. on the protection of personal data and on amending and supplementing certain acts (the "**Slovak Data Protection Act**") implementing the GDPR, which became effective as of 25 May 2018.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions provided by the GDPR apply.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (similar to the CNIL in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the GDPR.

The GDPR creates the concept of "**lead supervisory authority**." Where there is cross-border processing of personal data (*ie* , processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by, and answer to, the supervisory authority for their main or single establishment, the so-called "lead supervisory authority."

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory. ead supervisory authority is therefore of somewhat limited use to multinationals.

The Data Protection Office of the Slovak Republic (the 'Slovak Office') is:

Úrad na ochranu osobných údajov Slovenskej republiky (Official Slovak Name)

Hraniná 12
820 07, *Bratislava* 27
Slovak Republic

The Slovak Office is the supervisory authority and is responsible for overseeing the Slovak Data Protection Act and the GDPR in Slovakia.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

There is no registration or notice obligation to the Slovak Office as supervisory authority required anymore.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

There is an online form on the website of the Slovak Office which should be completed in order to notify the supervisory authority of the appointment of a DPO.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be:

- Processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle")
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle")
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- Accurate and where necessary kept up to date (the "accuracy principle")
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle")
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle")

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance for potentially years after a particular decision relating to processing personal data was rendered. Record-keeping, auditing and appropriate governance will all play a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject

- Where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law. (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to re-purpose personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymisation

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data

- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg*, commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they

demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

1. Necessary for entering into or performing a contract
2. Authorised by EU or Member State law
3. The data subject has given their explicit (*ie*, opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Collection and processing of personal data is governed by the GDPR.

However, there is specific regulation in this respect in the fourth part of the Slovak Data Protection Act. Pursuant to Section 78 of the Slovak Data Protection Act, these specific situations are as follows:

- a controller may process personal data without the consent of a data subject if the processing of personal data is necessary for academic, artistic or for literary purposes;
- a controller may process personal data without the consent of a data subject if the processing of personal data is necessary for the purposes of informing the public by means of mass media and if the personal data are processed by a controller which is authorised to do such business activity;
- a controller who is the employer of a data subject is authorized to provide his / her personal data or to make public his / her personal data in the scope of academic title, name, surname, position, personal employee´s number, department, place of work performance, telephone number, fax number, work email address and the identification details of employer, if this is necessary in connection with the performance of the employment duties of a data subject. Such provision of personal data or making them public shall not interfere with the reputability, dignity and security of a data subject;
- in the processing of personal data, a birth number may be used for the purpose of identifying a natural person only if its use is necessary for the purpose of processing. A data subject shall grant the explicit consent. Processing of a birth number on the legal basis of consent of a data subject shall not be excluded by a special regulation. Making public a birth number is prohibited; this does not apply if a data subject makes public a birth number;
- a controller may process genetic, biometric and health-related data on the legal basis of a special regulation or an international treaty to which the Slovak Republic is bound;
- if a data subject is dead, the consent required may be given by a close person. The consent is not valid if at least one close person has disagreed in writing.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU - U.S. Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

Pursuant to the GDPR, the free movement of personal data between the Slovak Republic and EU Member States is guaranteed; the Slovak Republic shall not restrict or prohibit the transfer of personal data in order to protect the fundamental rights of natural persons, in particular their right to privacy in connection with the processing of their personal data.

The transfer of personal data to third countries or international organisations is governed by the GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for

ensuring the security of the processing.

Controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The rights and obligations in regard to the security of personal data are governed by the GDPR.

In this respect, the Slovak Office issued Decree No. 158/2018 Coll. on Procedure when Assessing the Impact on the Protection of Personal Data as of 29 May 2018.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay. (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach. (Article 33(2)).

The notification to the supervisory authority must include where possible:

- The categories and approximate numbers of individuals and records concerned
- The name of the organisation's data protection officer or other contact
- The likely consequences of the breach and the measures taken to mitigate harm

Controllers are also required to keep a record of all data breaches (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Breach notifications are governed by the GDPR.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some

circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The Slovak Office has various powers to ensure compliance with the Slovak Data Protection Act and the GDPR.

For example, the Slovak Office is entitled to:

- on request, provide information to a data subject in relation to the exercise of her / his rights;
- order a controller or a processor to provide the necessary information;
- order a data controller to notify a data subject of a personal data breach;
- enter the premises of a controller or a processor;

- impose a corrective measure or a fine.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

In general, unsolicited electronic marketing requires prior opt-in consent. The opt-in requirement is waived under the 'same service/product' exemption. The exemption concerns marketing emails related to the same products/services as previously purchased from the sender by the user provided that:

- the user has been informed of the right to opt-out prior to the first marketing email
- the user did not opt-out, and
- the user is informed of the right to opt-out of any marketing email received. The exemption applies to electronic communication such as electronic text messages and email but does not apply with respect to communications sent by fax.

Direct marketing emails must not disguise or conceal the identity of the sender.

Pursuant to the GDPR, where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

Electronic marketing shall be in particular governed by Act No. 351/2011 Coll. on Electronic Communications, as amended (the "**ECA**").

Under the ECA, processing of the traffic data of a subscriber or user for the purposes of marketing services or the purposes of ensuring value added services by any public network or service providers is possible solely with the prior consent of the subscriber or the user. Prior to obtaining the consent, the public network or service providers are obliged to inform the subscriber or user on:

- the type of the traffic data processed;
- the purpose of the traffic data processing, and
- the duration of the data processing.

For the purposes of direct marketing, the call or use of automatic calls and communications systems without human

intervention, facsimile machines, e-mail, including SMS messages to the subscriber or user, who is a natural person, is allowed solely with his/her prior consent. Such consent must be provable. Users or subscribers are entitled to withdraw such consent at any time.

The prior consent of the recipient of a marketing e-mail shall not be required in the case of direct marketing of similar products and the services of a person, that has obtained electronic contact information of the recipient from the previous sale of its own product and/or service to such recipient and in line with the provisions of the ECA.

The recipient of an e-mail shall be entitled to refuse at anytime, by simple means and free, of charge such use of electronic contact information at the time of its collection and on the occasion of each message delivered where the recipient has not already refused such use.

Both,

- sending e-mails for the purposes of direct marketing without the determination of a valid address to which the recipient may send a request that he/she is no longer willing to receive such communication, and
- encouragement to visit a website in contradiction with a special regulation,

shall be prohibited.

ONLINE PRIVACY

As regards the protection of privacy and protection of personal data processed in the electronic communications sector, the provisions of the ECA shall apply. The ECA implemented e.g. Directive 2002/58/EC (as amended by Directive 2009/136/EC).

Under the ECA, the public network or service provider is obliged to ensure technically and organisationally the confidentiality of the communications and related traffic data, which are conveyed by means of its public network and public services. In particular recording, listening, or storage of data (or other kinds of an interception or a surveillance of communications and data related thereto) by persons other than users, or without the consent of the concerned users, shall be prohibited. However, this does not prohibit the technical storage of data, which is necessary for the conveyance of communications. However, the principle of confidentiality shall still apply.

Further to this, the network or service provider ('undertaking company') shall not be held liable for the protection of the conveyed information if such information can be directly listened to or obtained at the location of the broadcasting and/or reception.

However, this ban does not apply to temporary recording and storing of messages and related traffic data if it is required:

- for the provision of value added services ordered by a subscriber or user;
- to prove a request to establish, change or withdraw the service, or
- to prove the existence or validity of other legal acts, which the subscriber, user or undertaking company has made.

Under the ECA, each person that stores or gains access to the information stored in the terminal equipment of a user must be authorised for such processing by the concerned user whose consent must be based upon exact and complete information regarding the purpose of such processing of the data. In this regard, also the use of the respective setting of the web browser or other computer programme is considered (implied) consent.

Traffic data

Traffic data qualifies as personal data. Providers of telecommunication services may collect and use the following traffic data to the following extent:

- the number or other identification of the lines in question or of the terminal

- authorisation codes, additionally the card number when customer cards are used
- location data when mobile handsets are used
- the beginning and end of the connection, indicated by date and time and, where relevant to the charges, the volume of data transmitted
- the telecommunications service used by the user
- the termination points of fixed connections, the beginning and end of their use, indicated by date and time and, where relevant to the charges, the volume of data transmitted, and
- any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes.

Stored traffic data may be used after the termination of a connection only where required to set up a further connection, for billing purposes or where the user has requested a connection overview.

The service provider may collect and use the customer data and traffic data of subscribers and users in order to detect, locate and eliminate faults and malfunctions in telecommunications systems. This applies also to faults that can lead to a limitation of availability of information and communications systems or that can lead to an unauthorized access of telecommunications and data processing systems of the users.

Otherwise, traffic data must be erased by the service provider without undue delay following termination of the connection.

Service providers have to inform the users immediately, if any faults of data procession systems of the users become known. Furthermore the service provider has to inform the users about measures for detecting and rectifying faults.

Location Data

Location Data qualifies as personal data. This data may only be processed as required for the provision of requested services and is subject to prior information of the user. For all other purposes, the user's informed consent must be obtained. According to Section 4a BDSG, 13 German Telemedia Act (TMG) this means that:

- the user's consent must be intentional, informed and clear. For this purpose the user must be informed on the type, the scope, the location and the purpose of data collection, processing and use including any forwarding of data to third parties
- the user's consent must be recorded properly
- the user must be able to access the content of his consent declaration any time. It is sufficient that such information is provided upon the users' request
- the user's consent must be revocable at all times with effect for the future.

Users must always be informed of the use of cookies in a privacy notice. Cookies may generally be used if they are required in order to perform the services requested by the user. Otherwise, users must be provided with an opt-out mechanism. For this purpose, information on the use of cookies together with a link on how to adjust browser settings in order to prevent future use is sufficient.

Germany has not yet taken any measures to implement the e-privacy directive. However, in February 2014 the German Federal Ministry of Economic declared that the European Commission considers the Cookie Directive as implemented in Germany. However, since the European Commission´s exact interpretation is not known, a final official clarification is awaited. It therefore remains to be seen whether an active opt in, e.g. by clicking on a pop up screen will be required in the future.

Different rules apply in the case of tracking technologies which collect and store a user's IP address. Since IP addresses qualify as personal data, their processing for tracking and marketing services requires active opt-in consent.

Traffic Data

Traffic Data can only be processed for the purpose of the conveyance of a communication on an electronic communications network or for the invoicing thereof. The Traffic Data related to subscribers or users may not be stored without the consent of the person concerned and the undertaking company is required, after the end of a communication transmission, without delay, to destroy or make anonymous such Traffic Data, except as provided otherwise by the ECA.

If it is necessary for the invoicing of the subscribers and network interconnection payments, the undertaking company is required to store the Traffic Data until the expiration of the period during which the invoice may be legally challenged or the claim for the payment may be asserted. The undertaking company is required to provide the Traffic Data to the Office of Electronic Communication and Postal Services or the court in the case of a dispute between undertaking companies or between an undertaking company and a subscriber. The scope of the stored Traffic Data must be limited to the minimum necessary.

Location Data

The undertaking company may process the Location Data other than the Traffic Data which relates to the subscriber or the user of a public network or public service only if the data are made anonymous or the processing is done with user consent, and in the scope and time necessary for the provision of the value added service. The undertaking company must, prior to obtaining consent, inform the subscriber or user of the Location Data other than Traffic Data which will be processed, on the type of Location Data to be processed, on the purpose and duration of the processing, and whether the data will be provided to a third party for the purpose of the provision of the value added service. The subscriber or user may revoke its consent for the processing of location data at any time.

Following the Judgment of the Court of Justice of the European Union on 8 April 2014 in the joined cases of Digital Rights Ireland (C-293/12) and Kärtner Landesregierung (C-594/12) which cancelled so called "data retention" Directive 2006/24/EC, Constitutional Court of Slovak Republic on 29 April 2015 issued a Judgement (PL. ÚS 10/2014-78) ("**Judgement**") upon which the Constitutional Court proclaimed the certain provisions of the ECA to be non-compliant with the provisions of the Constitution of Slovak Republic, provisions of the Charter of Fundamental Rights and Freedoms and with the provisions of the Convention for the Protection of Human Rights and Fundamental Freedoms. Upon the Judgment, the obligation of the telecommunications operators to retain the Traffic Data and Location Data about the electronic communication of all citizens for the prescribed period (6/12 months) was abolished and removed from ECA.

KEY CONTACTS

JUDr. Dr. Michaela Stessl
Country Managing Partner
T +421 2 59202 122
michaela.stessl@dlapiper.com

Eva Skottke
Senior Associate
T +421 2 59202 111
eva.skottke@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SLOVENIA

Last modified 10 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The new Slovenian Data Protection Act (ZVOP-2) that will implement certain aspects of the GDPR has still not been adopted. It entered the legislative procedure in April 2018 (latest available version), but the Slovenian parliament was dissolved due to a general election so all legislative procedures were stopped. It is unclear what the final outcome will be or when the final act will be adopted (expected in autumn 2018). A new government has been formed, but it is still unclear when the new Data Protection Act will be adopted.

The current draft mostly follows the GDPR and only amends a few aspects, mostly of a systemic and procedural nature and adds some provisions in areas where GDPR allows to do so. We have to note that the academia and other stakeholders have voiced their concerns regarding the suitability of the current draft. Based on this, it is expected that the draft will undergo further major revisions. Furthermore, the new government may pursue a different policy regarding data protection which could cause further revisions.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for

"identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organisations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are

(Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor

and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU - U.S. Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and

freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Direct marketing by means of electronic communications is regulated by the Consumer Protection Act (*Zakon o varstvu potrošnikov* , Official Gazette 98/04 et seq.), the Electronic Commerce Market Act (*Zakon o elektronskem poslovanju na trgu*, Official Gazette 19/15), the Electronic Communications Act (*Zakon o elektronskih komunikacijah*, Official Gazette no. 109/12 et seq.) and the Personal Data Protection Act.

The consent of an individual is required for the purposes of electronic marketing. Direct marketing is allowed where the "similar service/product" exemption applies, however customers must be given clear and distinct opportunity to refuse the use of their electronic mail address at the time of the collection of these contact details, and on the occasion of every message in the event that the customer has not initially refused such use. Additionally, the sending of electronic mail for the purposes of direct marketing, which disguises or conceals the identity of the sender, or is sent without a valid address, is prohibited.

ONLINE PRIVACY

Traffic data

Traffic Data must be erased or made anonymous as soon as it is no longer needed for the purpose of the transmission of a communication, except in cases where a longer period of retention is statutory allowed. Nevertheless, an operator may, until complete payment for service is made but no later than by expiry of the limitation period, retain and process traffic data required

for the purposes of calculation and of payment relating to interconnection.

Location data

Location Data may only be processed for the purposes of providing the value-added service and when it is made anonymous, or with the prior consent of the user or subscriber, who may withdraw this consent at any time. Prior to issuing consent, a user or subscriber must be informed on (i) the possibility of refusing consent, (ii) the type of data to be processed, (iii) the purpose and duration of processing, and (iv) the possibility of the transmission of location data to a third party for the purpose of providing the value-added service.

Cookie compliance

The Electronic Communications Act (ZEKom-1) provides rules on the usage of cookies and similar technology for data storage.

Pursuant to ZEKom-1 the retention of information or the gaining of access to information stored in a subscriber's or user's terminal equipment (cookies) is only permitted if the subscriber or user gave their informed consent after having been given clear and comprehensive information about the information manager and the purpose of the processing of this information. However, an exception is provided in case of carrying out the transmission of a communication over an electronic communications network, or if this is strictly necessary for provision of service of information society explicitly requested by the subscriber or user.

KEY CONTACTS

Dr. Jasna Zwitter-Tehovnik
Partner
T +43 1 531 78 1042
jasna.zwitter-tehovnik@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SOUTH AFRICA

Last modified 28 January 2019

LAW

The right to privacy is recognized as a fundamental human right in the Bill of Rights of the Constitution of the Republic of South Africa and is protected in terms of the Constitution and the common law. This right to privacy is not absolute and may be limited where it is reasonable and justifiable to do so.

The Protection of Personal Information Act 4 of 2013 (POPIA) has been enacted, but only certain provisions are in effect at this time, with remaining provisions expected to take effect in 2019. While not fully in effect, POPIA is generally regarded as being a codification of the current common law position in South Africa. Once POPIA is in effect, it will specifically regulate the processing of personal information that is entered into a record pertaining to natural living persons as well as existing legal persons and there will be a one-year grace period for compliance.

Currently, the only sections of POPIA in force are those relating to establishing the office of the Information Regulator (the regulatory authority), the powers to make regulations to give effect to POPIA, and the definitions sections. The Information Regulator has been appointed and has published the Regulations to POPIA, which will come into effect when POPIA comes into effect.

DEFINITIONS

Definition of personal data

"Personal information" is defined in POPIA as information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing, juristic person, including:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin; color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief; culture, language and birth of the person
- Information relating to the education, medical, financial, criminal or employment history of the person
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person
- The biometric information of the person
- The personal opinions, views or preferences of the person
- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence

- The views or opinions of another individual about the person
- The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person

POPIA applies to the processing of personal information entered in a record by or for a responsible party / data controller that is domiciled in South Africa and that makes use of automated or non-automated means to process the personal information. It would also apply if the responsible party is not domiciled in South Africa but makes use of automated or non-automated means in South Africa unless those means are used only to forward personal information through South Africa.

POPI does not apply to the processing of personal information:

- In the course of a purely personal or household activity
- That has been de-identified to the extent that it cannot be re-identified again
- By or on behalf of the State with regard to national security, defense or public safety, or the prevention, investigation or proof of offenses; or for the purposes of the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information
- For exclusively journalistic purposes by responsible parties who are subject to, by virtue of office, employment or profession, a code of ethics that provides adequate safeguards for the protection of personal information
- Solely for the purposes of journalistic, literary or artistic expression to the extent that such exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression
- By Cabinet and its committees, the Executive Council of a province and a Municipal Council of a municipality
- For purposes relating to the judicial functions of a court referred to in section 166 of the Constitution, and
- Under circumstances that have been exempted from the application of the conditions for lawful processing by the Information Regulator in certain circumstances

Definition of sensitive personal data

Special personal information is information concerning religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information and criminal behavior (to the extent that such information relates to the alleged commission of an offense or any proceedings in respect of any offence allegedly committed, or the disposal of such proceedings).

Subject to certain prescribed exceptions, the processing of special personal information without the consent of the data subject is generally prohibited under POPIA.

NATIONAL DATA PROTECTION AUTHORITY

The first members of the Information Regulator have been appointed, with effect from December 1, 2016.

The powers, duties and functions of the office of the Information Regulator include providing education regarding the protection and processing of personal information; monitoring and enforcing compliance with the provisions of POPIA; consulting with interested parties and acting as mediator; receiving, investigating and attempting to resolve complaints; issuing enforcement notices and codes of conduct; and facilitating cross-border cooperation.

REGISTRATION

Data protection officers (referred to in POPI as "information officers") must be registered with the Information Regulator.

The responsible party is required to obtain prior authorization from the Information Regulator before processing personal information in certain circumstances prescribed in section 57 of POPIA, for example, where special personal information or personal information of children is transferred to locations that do not have adequate data protection laws and where information on criminal behavior or unlawful or objectionable conduct is processed on behalf of third parties. The responsible party is not otherwise required to register its processing of personal information.

DATA PROTECTION OFFICERS

Data protection officers (referred to in POPIA as "information officers") must be registered with the Information Regulator, once POPIA is in effect. The duties and responsibilities of a responsible party's information officer are set forth in POPIA and include encouraging and ensuring compliance with POPIA; dealing with any requests made to that responsible party in terms of POPIA; and working with the Information Regulator in respect of investigations by the Information Regulator in relation to that responsible party. The Regulations to POPIA, among other things, further provide that the information officer must ensure that a compliance framework is developed, implemented, monitored and maintained, and that a personal information impact assessment is conducted to ensure that adequate measures and standards exist.

COLLECTION & PROCESSING

"Processing" of information is defined in POPIA as any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

- The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use
- Dissemination by means of transmission, distribution or making available in any other form
- Merging, linking, as well as blocking, degradation, erasure or destruction of information

POPIA prescribes the following eight conditions for lawful processing of personal information:

- Accountability: The responsible party must comply with all the conditions for lawful processing.
- Purpose specification: Personal information must only be collected for a specific, explicitly defined lawful purpose related to a function or activity of the responsible party.
- Processing limitation: Processing must be justified on a ground recognized under POPIA (*eg*, consent/legitimate interests of the data subject, responsible party or the third party to whom the information is supplied).
- Further processing limitation: Processing must be in accordance with or compatible with the purpose for which it was initially collected subject to limited exceptions.
- Information quality: Steps must be taken to ensure that the information is complete, accurate, not misleading and updated where necessary.
- Openness: Notification requirements must be complied with when collecting personal information.
- Security safeguards: Appropriate, reasonable technical and organizational measures must be implemented and maintained to prevent loss of, damage to or unauthorized destruction of or unlawful access to personal information.
- Data subject participation: Data subjects have the right to request details of the personal information that a responsible party holds about them and, in certain circumstances, request access to such information.

TRANSFER

POPIA caters for two scenarios relating to the transfer of personal information, namely where a responsible party in South Africa

sends personal information to another country to be processed and where a responsible party in South Africa processes personal information that has been received from outside South Africa.

Receiving personal information from other countries

The requirements for the processing of personal information prescribed in POPIA will apply to any personal information processed in South Africa, irrespective of its origin.

Sending personal information to other countries for processing

A responsible party in South Africa may not transfer personal information to a third party in another country unless:

- The recipient is subject to a law, binding corporate rules or a binding agreement which:
    - Upholds principles for reasonable processing of the information that are substantially similar to the conditions contained in POPIA and
    - Includes provisions that are substantially similar to those contained in POPIA relating to the further transfer of personal information from the recipient to third parties who are in another country
- The data subject consents to the transfer
- The transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request or
- The transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request or
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party, or the transfer is for the benefit of the data subject and:
    - It is not reasonably practicable to obtain the consent of the data subject to that transfer, and
    - If it were reasonably practicable to obtain such consent, the data subject would be likely to give it

SECURITY

Section 19 of POPI places an obligation on a responsible party to secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss, damage to, or unauthorised destruction of; and unlawful access to, personal information.

To comply with this obligation, the responsible party must take reasonable measures to do all of the following:

- Identify all reasonably foreseeable internal and external risks to personal information under its control
- Establish and maintain appropriate safeguards against the risks identified
- Regularly verify that the safeguards are effectively implemented
- Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards

The responsible party must also have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

BREACH NOTIFICATION

In terms of section 22 of POPIA, where there are reasonable grounds to believe that the personal information of a data subject

has been accessed or acquired by any unauthorized person, the responsible party must notify the Information Regulator and the data subject, unless the identity of such data subject cannot be established.

The notification must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offenses or the Information Regulator determines that notification will impede a criminal investigation by the public body concerned and must be in writing and communicated to the data subject in a prescribed manner.

The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including all of the following:

- A description of the possible consequences of the security compromise
- A description of the measures that the responsible party intends to take or has taken to address the security compromise
- A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise
- If known to the responsible party, the identity of the unauthorized person who may have accessed or acquired the personal information

The Information Regulator may direct a responsible party to publicize, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Information Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

An operator / data processor is not required to notify the Information Regulator or data subjects where there are reasonable grounds to believe that there has been a data breach. It must, however, notify the responsible party/data controller of the suspected data breach.

ENFORCEMENT

Any person may submit a complaint to the Information Regulator alleging non-compliance with POPIA. The Information Regulator may also initiate an investigation into interference with the protection of personal information.

Upon receipt of a complaint, the Information Regulator may, inter alia, conduct a pre-investigation or full investigation of the complaint, act as conciliator, refer the complaint to another regulatory body if the Information Regulator considers that the complaint falls more properly within the jurisdiction of the other regulatory body, or decide to take no further action.

The Information Regulator's powers, for purposes of investigating a complaint include the power to summons and enforce the appearance of persons before the Information Regulator to give evidence or produce records or things; enter and search the premises occupied by a responsible party; and conduct interviews and inquiries.

If the Information Regulator is satisfied that a responsible party has interfered or is interfering with the protection of the personal information of a data subject it my issue an enforcement notice prescribing action to be taken by the responsible party to remedy the situation.

A responsible party who fails to comply with an enforcement notice is guilty of an offense and is, liable, on conviction, to a fine or imprisonment (or both) for a period of no longer than ten years (in terms of section 107), or alternatively to an administrative fine (in terms of section 109). Currently, the maximum fine under sections 107 and 109 of POPIA is R10 million although this may change once the regulations are promulgated.

Section 99 also makes provision for a civil action for damages resulting from non-compliance with POPIA.

ELECTRONIC MARKETING

The Electronic Communications and Transactions Act, 2002 (ECTA) and the Consumer Protection Act, 2008 empower consumers to restrict unwanted direct marketing. Under these laws, a data subject must be given the opportunity to opt out of receiving marketing information, free of charge.

Once POPIA comes into effect, the provisions in ECTA relating to marketing will be repealed and direct marketing will be regulated by POPIA whereby the opt-in regime will take effect. Under the POPIA, the processing of a data subject's personal information for the purposes of direct marketing is prohibited unless the data subject has given its consent, or the email recipient is a customer of the responsible party. The responsible party may only approach a data subject once in order for the data subject to opt in to receive marketing information. The Regulations to POPIA contain a prescribed form to be used when seeking this opt-in.

When sending emails to a data subject who is an existing customer: (a) the responsible party must have obtained the details of the data subject through a sale of a product or service; (b) the marketing should relate to its own similar products or services; and (c) the data subject must have been given a reasonable opportunity to opt out, free of charge, of the use of its personal information for marketing when such information was collected and on each occasion that marketing information is sent to the data subject, if the data subject has not initially refused the use of the personal information for electronic marketing purposes.

ONLINE PRIVACY

There are no sections of POPIA that regulate privacy in relation to cookies and location data. These issues may be dealt with in subsequent regulations or codes of conduct to be issued by the Information Regulator.

KEY CONTACTS

DLA Piper

Savanna Stephens
Associate
T +27 11 302 0830
savanna.stephens@dlapiper.com

Monique Jefferson
Director
T +27 11 302 0853
monique.jefferson@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SOUTH KOREA

Last modified 26 January 2017

LAW

In the past, South Korea did not have a comprehensive law governing data privacy. However, a law relating to protection of personal information (Personal Information Protection Act, 'PIPA') was enacted and became effective as of 30 September 2011.

Moreover, there is sector specific legislation such as:

- the Act on Promotion of Information and Communication Network Utilisation and Information Protection ('IT Network Act') which regulates the collection and use of personal information by IT Service Providers, defined as telecommunications business operators under Article 2.8 of the Telecommunications Business Act; and other persons who provide information or intermediate the provision of information for profit by utilising services rendered by a telecommunications business operator

- the Use and Protection of Credit Information Act ('UPCIA') which regulates the use and disclosure of Personal Credit Information, defined as credit information which is necessary to determine the credit rating, credit transaction capacity, etc. of an individual person. The UPCIA primarily applies to Credit Information Providers/Users, defined under Article 2.7 of the UPCIA as a person (entity) prescribed by Presidential Decree thereof who provides any third party with credit information obtained or produced in relation to his/her own business for purposes of commercial transactions, such as financial transactions with customers, or who has been continuously supplied with credit information from any third party to use such information for his/her own business, and

- the Act on Real Name Financial Transactions and Guarantee of Secrecy ('ARNFTGS') which applies to information obtained by financial or financial services institutions.

Under PIPA, except as otherwise provided for in any other Act, the protection of personal information shall be governed by the provisions of PIPA.

DEFINITIONS

Definition of personal data

Under PIPA, information pertaining to a living individual, which contains information identifying a specific person with a name, a national identification number, images, or other similar information (including information that does not, by itself, make it possible to identify a specific person but that which enables the recipient of the information to easily identify such person if combined with other information).

Under the IT Network Act, information pertaining to a living individual, which contains information identifying a specific person with a name, a national identification number, or similar in a form of code, letter, voice, sound, image, or any other form (including information that does not, by itself, make it possible to identify a specific person but that enables such person to be identified

easily if combined with other information).

The relevant Korean authorities' understanding is that the construction of Personal Data under PIPA and that under IT Network Act are the same in spite of subtle differences in definition wordings.

Definition of sensitive personal data

Under PIPA, Sensitive Personal Data is defined as Personal Data consisting of information relating to a living individual's:

- thoughts or creed
- history regarding membership in a political party or labour union
- political views
- health care and sexual life, and
- other Personal Data stipulated under the Enforcement Decree (the Presidential Decree) which is anticipated to otherwise intrude seriously upon the privacy of the person.

The Enforcement Decree of PIPA includes genetic information and criminal record as Sensitive Personal Data. The IT Network Act also has a similar definition.

NATIONAL DATA PROTECTION AUTHORITY

The Ministry of the Interior ("MOI") is in charge of the execution of PIPA. The Korea Communications Commission ('KCC') is in charge of the execution of the IT Network Act.

REGISTRATION

Under PIPA, a public institution which manages a Personal Data file (collection of Personal Data) shall register the following with the MOI:

- name of the Personal Data file
- basis and purpose of operation of the Personal Data file
- items of Personal Data which are recorded in the Personal Data file
- the method to process Personal Data
- period to retain Personal Data
- person who receives Personal Data generally or repeatedly, and
- other matters prescribed by Presidential Decree. A 'public institution' in this context refers to any government agency or institution.

The Presidential Decree of PIPA stipulates that the followings also shall be registered with the MOI:

- the name of the institution which operates the Personal Data file
- the number of subjects of the Personal Data included in the Personal Data file
- the department of the institution in charge of Personal Data processing

- the department of the institution handling the Personal Data subjects' request for inspection of Personal Data, and
- the scope of Personal Data inspection of which can be restricted or rejected and the grounds therefore.

Only 'public institutions' are required to register with the MOI.

DATA PROTECTION OFFICERS

Under PIPA, every Data Handler (which means any person, any government entity, company, individual or other person that, directly or through a third party, handles Personal Data in order to manage Personal Data files for work purposes) must designate a data protection officer.

Under the IT Network Act, every IT Service Provider must designate a director or chief officer of the department in charge of handling Personal Data as a data protection officer. Pursuant to Presidential Decree of the IT Network Act where, an IT Service Provider has less than 5 employees, the owner or representative director shall be the person in charge.

There are no nationality or residency requirements for the data protection officer. In the event that a data protection officer is not designated, the Data Handler may be subject to a maximum administrative fine of KRW 10 million under the PIPA or KRW 20 million under the IT Network Act.

COLLECTION & PROCESSING

If a Data Handler under PIPA or an IT Service Provider under the IT Network Act intends to collect Personal Data from the data subject or IT service user, it must:

- first notify the data subject or IT service user of the vital information stipulated under the law, and
- obtain the data subject's or IT service user's prior consent to such collection other than some exceptional cases stipulated under the law.

If a Data Handler under PIPA intends to collect Sensitive Personal Information, the consent must be separately obtained.

Under the amended IT Network Act, which became effective as of 18 August 2012, an IT Service Provider shall not collect a Resident Registration number (equivalent to Social Security number in the United States), unless:

- the IT Service Provider is designated as an identification institution by the KCC, or
- there exist special provisions under any other laws or Notification of the KCC.

Under the PIPA, prior to obtaining the prerequisite consent for collecting Personal Data from a data subject, a Data Handler must notify the data subject of:

- the purpose of collection and use of Personal Data
- items of Personal Data to be collected
- time period for possession and use of Personal Data, and
- the fact that the data subject has the right to refuse to consent and the consequences of refusing.

Under the IT Network Act, prior to obtaining prerequisite consent for collecting Personal Data from an IT service user, an IT Service Provider must notify the IT service user of:

- the purpose of collection and use of Personal Data
- items of Personal Data to be collected, and

- time period for possession and use of Personal Data.

Under the newly amended PIPA, effective as of 7 August 2014, an Data Handler shall not handle a Resident Registration number, unless:

- there exists special provisions requiring or permitting the handling of the Resident Registration number under other laws
- there is clear evidence of some urgent need to handle the data, for the sake of the safety or property of the data subject or of a third party, or
- the handling of the Resident Registration number is unavoidable and there exist special provisions under ordinance of the MOI.

When a certain business transfer occurs, the Data Handler or IT service provider must provide its data subjects or IT service users a chance to opt out by providing a notice, including items of:

- the expected occurrence of Personal Data transfers
- the contact information of the recipient of the Personal Data, including the name, address, telephone number and other contact details of the recipient, and
- the means and process by which the data subject or IT service user may refuse to consent to the transfer of Personal Data.

If the data subject or IT service user is under 14, the consent of his/her legal guardian must be obtained.

As a general rule, a Data Handler under PIPA or an IT Service Provider under the IT Network Act may not handle Personal Data without obtaining the prior consent of the data subject or IT service user, beyond the scope necessary for the achievement of the Purpose of Use. This general rule also applies where a Data Handler or IT Service Provider acquires Personal Data as a result of a merger or acquisition.

Exceptions to the general rule above apply in the following cases under PIPA:

- where there exist special provisions in any Act or it is inevitable to fulfil an obligation imposed by or under any Act and subordinate statute
- where it is inevitable for a public institution to perform its affairs provided for in any Act and subordinate statute
- where it is inevitably necessary for entering into and performing a contract with a subject of Personal Data
- where it is deemed obviously necessary for the physical safety and property interests of a subject of Personal Data or a third person when the subject of Personal Data or his/her legal representative cannot give prior consent because he/she is unable to express his/her intention or by reason of his/her unidentified address, and
- where it is necessary for a Data Handler to realise his/her legitimate interests and this obviously takes precedence over the rights of a subject of Personal Data. In such cases, this shall be limited to cases where such data is substantially relevant to a Data Handler's legitimate interests and reasonable scope is not exceeded.

Exceptions to the general rule above apply in the following cases under the IT Network Act:

- if the Personal Data is necessary in performing the contract for provision of IT services, but it is obviously difficult to get consent in an ordinary way due to any economic or technical reason.
- if it is necessary in settling the payment for charges on the IT services rendered, and

- if a specific provision exists in this Act or any other Act.

Under the ARNFTGS, financial institutions must obtain written consent for the disclosure of an individual's information relating to his/her financial transactions.

TRANSFER

As a general rule, a Data Handler or an IT Service Provider may not provide Personal Data to a third party without obtaining the prior opt in consent of the data subject or IT service user.

Exceptions to the general rule above apply in the following cases under PIPA:

- where there exist special provisions in any Act or it is necessary to fulfil an obligation imposed by or under any Act and subordinate statute
- where it is necessary for a public institution to perform its affairs provided for in any Act and subordinate statute, etc, and
- where it is deemed obviously necessary for the physical safety and property interests of a subject of Personal Data or a third person when the subject of Personal Data or his/her legal representative cannot give prior consent because he/she is unable to express his/her intention or by reason of his/her unidentified address, etc.

Exceptions to the general rule above apply under the IT Network Act if a specific provision exists in this Act or any other act otherwise.

Under PIPA, a Data Handler must obtain consent after it notifies the data subject of:

- the person (entity) to whom the Personal Data is furnished
- purpose of use of the Personal Data by the person (entity)
- types of Personal Data furnished
- period of time during which the person (entity) will possess and use the Personal Data, and
- the fact that the data subject has the right to refuse to consent and the consequences of refusing.

Under the IT Network Act, an IT Service Provider must notify the IT service user of:

- the person (entity) to whom the Personal Data is furnished
- purpose of use of the Personal Data by the person (entity)
- types of Personal Data furnished, and
- period of time during which the person (entity) will possess and use the Personal Data, and then obtain consent from the IT service user.

The UPCIA stipulates that prior to obtaining prerequisite consent for providing personal credit information to any other person, a Credit Information Provider/User must notify the credit information subject of:

- the person (entity) to whom the credit information will be furnished
- the purpose of use of the Personal Credit Information by the person (entity)
- the types of Personal Credit Information to be furnished, and

- the period of time during which the person (entity) will possess and use the Personal Credit Information.

Exceptions to the general rule above apply in the following cases under the UPCIA:

- where a Credit Information Company as defined under Article 2.5 of the UPCIA provides such information for the purpose of performing central management and utilisation thereof with another Credit Information Company or Credit Information Collection Agency as defined under Article 2.6 of the UPCIA
- where such provision is required to perform a contract, and to entrust the processing of credit information under Article 17.2 of the UPCIA
- where the relevant Personal Credit Information is provided as part of rights and obligations that are transferred by way of business transfer, division, merger, etc
- where Personal Credit Information is provided for a person who uses the information for purposes prescribed by Presidential Decree, including claims collection (applicable only to the credit which is an object of collection), license and authorisation, determination of a company's credit worthiness, and transfer of securities
- where Personal Credit Information is provided in accordance with a court order for submission thereof or a warrant issued by a judicial officer
- where such information is provided upon the request of a prosecutor or judicial police officer, in the event of occurrence of an emergency where a victim's life is in danger or he/she is expected to suffer bodily injury, etc., so that no time is available to issue a judicial warrant
- where such information is provided as the head of a competent government office requests, in writing, for the purpose of inquiry and examination in accordance with any laws pertaining to taxes or demands the taxation data required to be provided in accordance with such laws pertaining to taxes
- where Personal Credit Information held by a financial institution is provided to a foreign financial supervisory body in accordance with international conventions, etc
- where information by which the credit worthiness of related persons, such as a violator of credit order prescribed by Presidential Decree, and an oligopolistic stockholder and the largest investor of an enterprise, can be determined, is provided; and
- where such information is otherwise provided in accordance with other laws.

Under the ARNFTGS, financial institutions must obtain written consent for the transfer of an individual's information relating to his/her financial transactions to a third party.

Under PIPA, when processing Personal Data acquired indirectly by way of a third party transfer, transferees who meet a certain threshold as provided by the Presidential Decree will be obligated to notify the data subject of (i) the third party source (transferor) from which the Personal Data was acquired, (ii) the intended use of the received Personal Data, and (iii) the fact that the data subject has the right to request for suspension from processing Personal Data.

SECURITY

Under PIPA and IT Network Act, every Data Handler or IT Service Provider must, when it handles Personal Data or Sensitive Personal Data of a data subject or IT service user, take the following technical and administrative measures in accordance with the guidelines prescribed by Presidential Decree to prevent loss, theft, leakage, alteration, or destruction of Personal Data:

- establishment and implementation of an internal control plan for handling Personal Data in a safe way

- installation and operation of an access control device, such as a system for blocking intrusion to cut off illegal access to Personal Data
- measures for preventing fabrication and alteration of access records
- measures for security including encryption technology and other methods for safe storage and transmission of Personal Data
- measures for preventing intrusion of computer viruses, including installation and operation of vaccine software, and
- other protective measures necessary for securing the safety of Personal Data.

BREACH NOTIFICATION

Under PIPA, if a breach of Personal Data occurs the Data Handler must notify the data subjects without delay of the details and circumstances, and the remedial steps planned. If the number of affected data subjects exceeds 10,000, the Data Handler shall immediately report the notification to data subjects and the result of measures taken to MOI, KISA or the National Information Security Agency ('NIA').

Under the IT Network Act, an IT Service Provider must, if it discovers an occurrence of intrusion:

- report it to the KCC or the Korea Internet & Security Agency (KISA) within twenty four (24) hours of knowledge of the intrusion, and
- analyse causes of intrusion and prevent damage from being spread, whenever an intrusion occurs.

The KCC may, if deemed necessary for analysing causes of an intrusion, order an IT Service Provider to preserve relevant data, such as access records of the relevant information and communications network.

Under the newly amended IT Network Act, which became effective as of 29 November 2014, if a loss, theft or leakage of Personal Data occurs, the IT Service Provider must notify the IT Service user immediately and report to the KCC within twenty four (24) hours of the details and circumstances, and the remedial steps planned.

ENFORCEMENT

The competent authorities may request reports on the handling of Personal Data, and also may issue recommendations or orders if a Data Handler or IT Service Provider violates PIPA or the IT Network Act. Non compliance with a request or violation of an order can result in fines, imprisonment, or both.

For example, MOI, the supervising authority for Data Handlers, can issue a corrective order in response to any breach of an obligation not to provide Personal Data to a third party. Breach of a corrective order leads to an administrative fine of not more than KRW 30 million. Prior to issuing a corrective order, MOI may take an incremental approach and instruct, advise and make recommendations to the Data Handler.

Under the IT Network Act, an IT Service Provider who collected Personal Data without consent of the relevant user shall be subject to the penalty of imprisonment for not more than 5 years or a fine not exceeding KRW 50 million.

Under the UPCIA, a Credit Information Provider/User who has provided Personal Credit Information without consent of the relevant credit information subject shall be subject to the penalty of imprisonment of up to 5 years or a fine not exceeding KRW 50 million.

Under the ARNFTGS, a person who discloses information or data concerning financial transactions shall be punished by imprisonment not exceeding 5 years or by a fine not exceeding KRW 30 million.

Punitive damages

In the event that a Credit Information Provider/User suffers any damages resulting from the Data Handler's conduct, the Credit Information Provider/User may bring a claim against the Data Handler for such damages. In such cases, a Data Handler may not be discharged from liability unless it can prove that there was no intentional act nor negligence on its part.

As of July 25, 2016, as a result of an amendment to PIPA, in instances Personal Data breaches caused by the Data Handler's intentional act or negligence, the Data Handler may be liable for three times the damages suffered.

ELECTRONIC MARKETING

Under the IT Network Act, anyone who intends to transmit an advertisement by information and communication network must receive the explicit consent of the individual, but if the individual either withdraws consent or does not give consent, then an advertisement with commercial purposes may not be transmitted.

In addition, the transmitter of advertisement information for commercial purposes must disclose the following specifically within the advertisement information:

- the identity and contact information of the transmitter; and
- instructions on how to consent or withdraw consent for receipt of the advertisement information.

A person who transmits an advertisement shall not take any of the following technical measures:

- a measure to avoid or impede the addressee's denial of reception of the advertising information or the revocation of his consent to receive such information
- a measure to generate an addressee's contact information, such as telephone number and electronic mail address, automatically by combining figures, codes, or letters
- a measure to register electronic mail addresses automatically with intent to transmit advertising information for profit, and
- various measures to hide the identity of the sender of advertising information or the source of transmission of an advertisement.

ONLINE PRIVACY

Cookie, log, IP information, etc. are also regulated by the IT Network Act as personal data, which if combined with other information enable the identification of a specific individual person easily. Under the IT Network Act, using cookies (or web beacons) must be done with the opt-out consent of the user and the privacy policy must publicise the matters concerning installation, operation and opt-out process for automated means of collecting personal information, such as cookies, logs and web beacons.

The protection of location information is governed by the provisions of the Act on the Protection, Use, etc. of Location Information ('LBS Act').

Under the LBS Act, any person who intends to collect, use, or provide location information of a person or mobile object shall obtain the prior consent of the person or the owner of the object, unless:

- there is a request for emergency relief or the issuance of a warning by an emergency rescue and relief agency
- there is a request by the police for the rescue of the person whose life or physical safety is in immediate danger, or
- there exist special provisions in any Act.

Under the LBS Act, any person (entity) who intends to provide services based on location information (the 'Location-based Service Provider') shall report to the KCC. Further, any person (entity) who intends to collect location information and provide

the collected location information to location-based service providers (the 'Location Information Provider') shall obtain a license from the KCC.

If a Location Information Provider intends to collect personal location information, it must specify the following information in its service agreement, and obtain the consent of the subjects of personal location information:

- name, address, phone number and other contact information of the Location Information Provider
- rights held by the subjects of personal location information and their legal agents and methods of exercising the rights
- details of the services the Location Information Provider intends to provide to Location-based Service Providers
- grounds for and period of retaining data confirming the collection of location information, and
- methods of collecting location information.

If a Location-based Service Provider intends to provide location-based services by utilising personal location information provided from a Location Information Provider, it must specify the following information in its service agreement, and obtain the consent of the subjects of personal location information:

- name, address, phone number and other contact information of the Location-based Service Provider
- rights held by the subjects of personal location information and their legal agents and methods of exercising the rights
- details of the Location-based Services
- grounds for and period of retaining data confirming the use and provision of location information, and
- matters concerning notifying the personal location information subject of the provision of location information to a third party as below.

If a Location-based Service Provider intends to provide location information to a third party, in addition to the above, it must notify the subjects of personal location information of the third party who will receive the location information and the purpose of this provision.

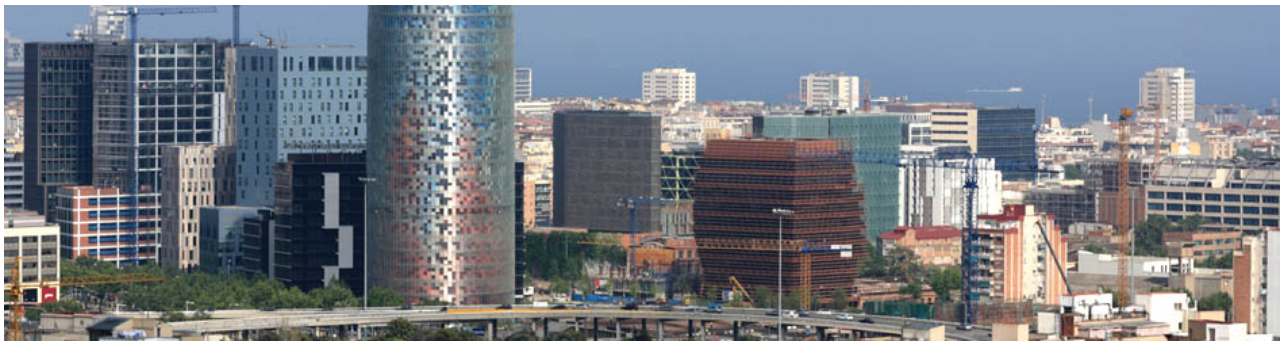
KEY CONTACTS

Daniel Lee
Partner
T +82 2 6270 8899
daniel.lee@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SPAIN



Last modified 14 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

After a very long delay and amidst rumors that the Spanish Parliament could be dissolved and early elections called, the Spanish Senate speedily dismissed all proposals for further changes and approved the new Spanish Fundamental Law on Data Protection and digital rights guarantee, which is in force from 7 December 2018 (**"NLOPD"**).

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal**

convictions and offences (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Spanish competent national supervisory authority is the *Agencia Española de Protección de Datos* **("AEPD")**, which also represents Spain on the European Data Protection Board.

The contact details of the AEPD are as follows:

- Address: C/Jorge Juan, 6, 28001 Madrid, Spain
- Telephone: +34 901 100 099/ +34 91 266 35 17
- Website: www.agpd.es

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain

comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The NLOPD includes a lengthy list of organisations and companies that are required to appoint a DPO. Accordingly, insurance or reinsurance companies, financial credit institutions, educational institutions, electric and natural gas distributors, and advertising and marketing companies, among others, are required to appoint a DPO. The NLOPD also allows organisations and companies to voluntarily appoint a DPO. Please note that, in either case, the appointment of the DPO must be communicated to the AEPD.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");

- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organisations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or

c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Data protection principles

The NLOPD foresees certain scenarios where the controller shall not be responsible for inaccurate data (provided it has taken all reasonable measures to ensure deletion or rectification without delay).

Criminal Convictions and Offences data

Article 10 of the NLOPD allows lawyers and legal entities to process the information provided by their clients related to criminal convictions and offences for the purposes of rendering the corresponding legal services.

Processing of administrative offence or penalties

The processing of personal data related to administrative offences or penalties is permitted if it is carried out by the relevant public bodies having sanctioning powers over such offenses, and only to the extent necessary for achieving their legitimate purposes. If those requirements are not met, the processing shall be allowed by an specific law, or be based on the data subject's consent.

Please note that lawyers and legal entities are also allowed to process the information provided by their clients related to administrative offenses or penalties for the purposes of rendering the corresponding legal services.

Credit Solvency Databases

The NLOPD sets out stringent requirements for including personal data on credit solvency databases. In this regard, the information to be provided to data subjects as well as the particularities of the debt are, among others, key aspects to be taken into account.

CCTV Processing

Under the NLOPD, the processing of images through CCTV is only permitted for security purposes, provided that (i) the data obtained is duly deleted within the corresponding period of time (unless it is relevant for evidence purposes), and (ii) the mandatory notice requirements are met.

Whistleblowing

The processing of personal data relating to whistleblowing (including anonymous reporting) is permitted provided that (i) employees are duly informed ,(ii) whistleblowing databases are only accessed by the necessary persons to carry out internal control purposes or to initiate the relevant disciplinary proceedings, and (iii) the data obtained is duly deleted within the mandatory period of time.

Unfair competition

The NLOPD generates a new catalogue of "unfair competition practices" linked to personal data.

Data processing for electoral purposes

Political parties, coalitions and electoral groups can use personal data obtained from websites and other public sources to carry out political activities during an election period. Likewise, sending electoral propaganda by electronic means, as well as contracting any such propaganda on social or similar networks will not be deemed a commercial activity.

Transparency (Privacy Notices)

The NLOPD allows provisions of the information required by Articles 13 and 14 of the GDPR in layers. In this sense, a first layer should include the "basic information" of the relevant processing as well as an immediate and easily accessible form (*i.e.*, a link) to the second layer, where the rest of information to be provided under Articles 13 and 14 of the GDPR shall be included. Please note that the content of the before-mentioned "basic information" depends on each case, but most of the times includes (i) the identity of the controller, (ii) the purpose of the processing, and (iii) the rights under Article 15 – 22 of the GDPR.

Rights of the data subject

Under the NLOPD, a data subject's right of access is deemed granted when the controller provides him/her with a means that permanently guarantees remote, direct and secure access to his/her personal data. In addition, the NLOPD indicates that more than one right of access request within six months shall be considered repetitive for the purposes of Article 12(5) of the GDPR unless the relevant requests are based on a legitimate reason.

Under the NLOPD, controllers must clearly indicate in their internal information systems the cases where the processing of personal data is restricted.

Blocking right / Blocking duty (NLOPD)

The NLOPD states that following the exercise of rectification or erasure, controllers shall "block" the personal data so that it shall remain available to the relevant public authorities in very specific situations. The NLOPD also offers other alternatives in case the "blocking" of personal data is not feasible or involves a disproportionate effort.

Rights of the deceased

The NLOPD recognizes the right to digital testament. Moreover, the heirs of the deceased are entitled to exercise the rights of access, erasure and rectification of data unless the deceased person would had prohibited it (or if it is not in line with applicable law).

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU - U.S. Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;

d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

According to the NLOPD, certain transfers to countries outside the EU require prior authorization from the AEPD

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In line with paragraph 1 above, the NLOPD includes an exhaustive list with certain scenarios that shall be particularly taken into account when adopting and implementing the corresponding technical and organizational measures.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and

freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Electronic Marketing is regulated in Spain, in addition to the Spanish Data Protection Act, by the Spanish Act on the Information Society Services and e-Commerce ('LSSI'), as amended in March 2012. The general principle is that deliveries of electronic marketing materials are lawful only if they have been explicitly authorised in advance by the recipients (authorisation that is required not just for individuals, but also where the recipient is a legal entity, broadening here the scope of Spanish Data Protection Act). An exception to this general principle applies to deliveries to clients when the materials refer to products/services that are equal or similar to the ones sold to them in the past by the company sponsoring the advertisement.

Electronic publicity shall:

- be clearly marked as such by means of the terms PUBLI or PUBLICIDAD placed inside the subject line,
- allow the recipient to opt-out at all times, even at the time of registration, and
- clearly identify the sponsor of the delivery. It is the sponsor of the delivery, not the electronic publicity company that shall be held liable in case of enforcement. Opt-out shall include an email address when the publicity was delivered by email too. Opt-out procedure shall be simple and free for the recipient of the publicity.

Enforcement shall include, inter alia, fines that, in most cases, shall be between EUR 30,000 and EUR 150,000.

The NLOPD states that databases containing the identification details of those data subjects who have expressed their opposition

to receiving commercial communications may be created. These databases must be reviewed by the entities sending commercial communications (the access details to these databases will be published by the AEPD) unless the relevant data subjects have previously granted their consent to receiving such commercial communications.

Finally, it shall also be taken into account that that the NLOPD permits processing activities where the purpose is to avoid sending commercial communications to those data subjects who have expressed their opposition to receiving them.

ONLINE PRIVACY

Cookies are regulated in Spain, in addition to the Spanish Data Protection Act, by the Spanish Act on the Information Society Services and e-Commerce ('LSSI'), as amended in March 2012. By the end of April 2013, the AEPD has released Guidance Notes on the use of cookies. Although the Guidance Notes are not legally binding they give useful indications on the best market practice and on the criteria that the AEPD would follow when enforcing the law.

The new regulation requires data controllers to inform cookies' recipients (referred to in the LSSI as giving users the 'actual opportunity') – including legal entities – of the existence and use of cookies, their scope and how to deactivate them. Actual opportunity is interpreted by the regulator as a procedure by which the user cannot browse the website, for example, without noticing the invitation to review the above-mentioned information and carrying out an active behaviour (even a simple one like pressing the ESC key) to continue browsing after being presented with the information or the opportunity to review it. A semi-transparent layer on the usual homepage screen is a generally approved mechanism to request the consent (although AEPD has indicated in some reports released in 2014 that a two-step warning approach may work best (first warning on the landing page containing the basics, second one on a separate cookies policy including full details). Certain types of cookies (eg session cookies) are exempt from these restrictions as per the WP29 criteria released during the summer of 2012. The Spanish AEPD has made known to the public, by the way of a resolution, that in some cases the delivery of cookies to the computer of a user based in Spain may trigger the application of Spanish Data Protection Act in full.

On location data, the local position is that it may be acceptable provided that:

- users are informed at all times on whether the location system is active
- users have agreed to be located, and
- users have the option (especially when being off-duty if the location data is used in an employment context) to turn off the system.

One of the main novelties of the NLOPD is that it accepts new "**digital rights**", including, *i.e.*, Internet neutrality, universal access to Internet, security of online communications, digital education, protection of minors on the Internet, amendment / update of non-accurate information on the Internet, a right to be forgotten-like right not to be found by search engines on the Internet and social networks.

On top of this, certain provisions of the NLOPD may have an impact on the relationship between a company and its employees (*i.e.*, monitoring of digital devices, digital disconnection of the employees outside working hours, privacy at the workplace).

KEY CONTACTS

Diego Ramos
Partner
T +349 17901658
diego.ramos@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SWEDEN

Last modified 14 January 2019

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Data Protection Act (2018:218) and the Data Protection Ordinance (2018:19) (the "DPA") - The DPA regulates general aspects of data protection where the GDPR allows, e.g. processing of social security numbers and processing of data pertaining to criminal offences. The DPA entered into force on 25 May 2018.

In addition to the Swedish DPA, a vast number of sector specific acts have been adopted in Sweden, for example relating to the sectors of healthcare, finance, energy, environment, education, referendums/elections, enterprise, communication, labour market, etc. On 4 April 2018 in a draft to a proposal to the Council on legislation relating to personal data for scientific research purposes, the Swedish government criticised the proposal for a new scientific research data act, meaning that an update of other acts (such as the Ethical Review Act) will be enough in order to complement the GDPR. As a result of this the Swedish parliament in November 2018 voted in favor of the proposed amendments to acts relating to the processing of personal data for scientific research purposes, which did not include the adoption of a new scientific research data act. The amendments to the relevant acts entered into force on 1 January 2019.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Swedish Data Protection Authority ("Datainspektionen"), Drottninggatan 29 5th Floor, Box 8114 104 20 Stockholm
Tel. +46 8 657 6100
datainspektionen@datainspektionen.se
www.datainspektionen.se

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or

processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

No derogations except that the Swedish Public Access to Information and Secrecy Act (2009:400) shall apply in relation to the confidentiality obligation of a DPO within the public sector, instead of article 37 GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");

- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organisations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or

c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

- In Sweden, data concerning personal identity numbers/social security numbers may be processed without consent only where manifestly justified having regard to the purpose of the processing the importance of secure identification or some other substantial reason.
- Criminal data (Art. 10 GDPR) may be processed by bodies other than public authorities only for the purposes of establishing, exercising or defending legal claims, or to comply with a legal obligation. The Swedish Datainspektionen (the supervisory authority) is entitled to prescribe further derogations to this provision.
- Swedish law may prohibit controllers to disclose certain data to data subjects. This applies to the rights in articles 13-15 in the GDPR.
- As regards personal data in text which has not been finalised (e.g. drafts) or memory notes, the right under article 15 in the GDPR will not apply. This exemption may, however, not be relied on by a data controller if such personal data (i) has been disclosed to a third party, (ii) is processed solely for archiving purposes in the public interest or for statistical purposes, or (iii) is processed in draft text for more than one year without being finalised.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU - U.S. Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised

or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

There are no specific security requirements set out in the DPA. However, it should be noted that certain security related provisions are prescribed under the Patient Data Act (2008:355) when processing personal data, regarding e.g. confidentialilty, access, and disclosure. Moreover, a two-factor authentication when accessing special categories of data over an open network and encryption where sending special categories of data are examples of previous recommendations from the Datainspektionen (the Swedish supervisory authority).

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

No derogations under Swedish law, except that personal data breaches that fall under the Swedish Criminal Data Act (2018:1177) shall be reported by public authorities separately in accordance certain provisions of the act.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to

receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.

- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

In relation to public authorities, administrative fines under the Swedish DPA may amount to maximum SEK 5 000 000 (in relation to Article 83(4) GDPR) and SEK 10 000 000 (in relation to Articles 83(5) and 83(6) GDPR).

Moreover, the DPA regulates procedural matters relating to decisions on administrative fines and how to appeal such decisions made by authorities (for example, the right to appeal to the Swedish Administrative Court).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Act applies to most electronic marketing activities, given that it is likely that such marketing involves processing of personal data (eg an e-mail address is likely regarded as personal data under the Act). Please note that if the data subject's e-mail address has not been obtained in the context of a customer relationship or similar, the data subject's consent is, as a main rule, required for electronic marketing. Moreover, a data subject has a right to at any time oppose ('opt-out' of) further processing of his or her personal data for marketing purposes.

There is no provision in the DPA which concerns in particular the processing of personal data in relation to electronic marketing.

There is, however, pre-existing legislation in Sweden (such as the Marketing Act (2008:486) and the Electronic Communications Act (2003:389)) implementing the EU Directive 2002/58/EC (the "ePrivacy Directieve") which regulates electronic marketing in Sweden.

Note that certain provisions relating to electronic marketing under Swedish law may be amended in the future due to the upcoming ePrivacy Regulation which will become immediately enforceable as law in all EU member states.

ONLINE PRIVACY

Pursuant to the Swedish Electronic Communications Act (as amended by e-Privacy Directive 2009/12/EC), a cookie may be stored on a user's terminal equipment, only if the user has been given access to information on the purpose of the processing and given his or her consent, ie the user must give his/her prior 'opt-in' consent before a cookie is placed on the user's computer. The government stated in the preparatory works to the Swedish Electronic Communications Act that the implementation of the new e-Privacy Directive should not be regarded as a material change. This has been construed by some that implied consent through browser settings shall be regarded as a valid consent under the Act, provided that sufficient information is given to the user eg in a cookie policy. This is, however, unclear and the Swedish Post and Telecom Authority has not issued any guidance in this regard.

Consent is, however, not required for cookies that are:

- used for the sole purpose of carrying out the transmission of communication over an electronic communications network, or
- necessary for the provision of a service explicitly requested by the user.

Wilful or negligent breach of the Swedish Electronic Communications Act in this regard is sanctioned with fines, provided that the offence is not sanctioned by the Swedish Criminal Code (Sw. *brottsbalken*). However, if the breach is deemed to be minor, no sanction shall be imposed. To our knowledge there has been no case where a website operator has been fined for breach of the Swedish Electronic Communications Act.

Sweden has set the digital age of consent as 13 in relation to information society services.

KEY CONTACTS

Johan Sundberg
Advokat/Partner
T +46 70 302 75 62
johan.sundberg@dlapiper.com

Johan Thörn
Senior Associate
T T +46 8 769 79 30
johan.thorn@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SWITZERLAND

Last modified 28 January 2019

LAW

The processing of personal data is mainly regulated by the Federal Act on Data Protection of June 19, 1992 (DPA) and its ordinances, *ie*, the Ordinance to the Federal Act on Data Protection (DPO) and the Ordinance on Data Protection Certification (ODPC).

In addition, the processing of personal data is further restricted by provisions in other laws, mainly with regard to the public sector and regulated markets.

It should be noted that the DPA is currently subject to a substantial revision. On September 15, 2017, the Federal Council published the final draft and the dispatch to the Federal Parliament regarding the new DPA. In the summer of 2018, the revision was split into two parts. The first part relates to the implementation of the EU Directive 2016/680 in the context of the Schengen/Dublin treaty and has no immediate impact on data subjects (as it is generally limited to the federal authorities' competencies in the context of administrative and judicial assistance in criminal matters). This part was passed by Parliament in September 2018 and is expected to come into force upon the end of the three-month referendum period on January 18, 2019.

The second part is the actual comprehensive revision of the DPA (based on the draft legislation of September 15, 2017). It will most likely be initially discussed in Parliament during the spring session 2019, and may be passed by Parliament in the autumn session of 2019, which will trigger the three-month referendum period. On this basis, the revised DPA (and the corresponding ordinance) is expected to enter into force no sooner than the beginning of 2020. The revision of the DPA aims to strengthen data protection in general and to align the DPA with the requirements of the EU General Data Protection Regulation (GDPR), in order to facilitate compliance of Swiss companies with those aspects of the GDPR that are applicable to controllers or processors outside of the EU, and to ensure that the EU will continue to consider Switzerland as providing an adequate level of data protection.

DEFINITIONS

Definition of personal data

Personal data means all information relating to an identified or identifiable natural or legal person. It should be noted that data relating to legal entities falls within the scope of current Swiss data protection law, as opposed to most EU members' data protection laws. The ongoing revision proposes to exempt data regarding legal entities from the scope of the DPA, and it seems likely that the proposal will be accepted in this respect.

Definition of sensitive personal data

Sensitive personal data is defined as data on:

- Religious, ideological, political or trade union related views or activities

- Health, the intimate sphere or racial origin
- Social security measures
- Administrative or criminal proceedings and sanctions

"Personality profiles" are protected to the same extent under the DPA as sensitive personal data. Personality profiles are collections of data that allow the appraisal of essential characteristics of the personality of an individual.

NATIONAL DATA PROTECTION AUTHORITY

Federal Data Protection and Information Commissioner (FDPIC)

Feldeggweg 1
CH - 3003 Berne
Switzerland

T +41 (0)58 462 43 95
F +41 (0)58 465 99 96

The FDPIC supervises federal and private bodies, advises and comments on the legal provisions on data protection and assists federal and cantonal authorities in the field of data protection.

The FDPIC informs the public about his findings and recommendations, and maintains and publishes the register for data files.

REGISTRATION

The processing of personal data by private persons does not usually have to be notified or registered, respectively. However, private persons must register their data files before the data files are opened, if:

- They regularly process sensitive personal data or personality profiles, or
- They regularly disclose personal data to third parties;

...and if none of the following exemptions applies:

- The data is processed pursuant to a statutory obligation.
- The Swiss Federal Council has exempted the particular processing from the registration requirement because it does not prejudice the rights of the data subjects (which the Swiss Federal Council has done in the ODP, inter alia, regarding data files from suppliers or customers, provided they do not contain any sensitive personal data or personality profiles).
- The data controller uses the data exclusively for publication in the edited section of a periodically published medium and does not pass on any data to third parties without informing the data subjects.
- The data is processed by journalists who use the data file exclusively as a personal work aid.
- The data controller has designated a data protection officer who independently monitors internal compliance with data protection regulations and maintains a list of the data files.
- The data controller has acquired a data protection quality mark under a certification procedure and has notified the FDPIC of the result of the evaluation.

DATA PROTECTION OFFICERS

There is no requirement under Swiss data protection law to appoint a data protection officer.

However, a data controller can be dispensed from registering its data files if it has designated a data protection officer who:

- Carries out his / her duties autonomously and independently
- Has a certain level of expertise that is appropriate for the relevant data processing at the company (whereas it is not relevant whether or not the respective expertise was acquired in Switzerland)
- Must check and audit the processing of personal data within the company
- Must be in a position to recommend corrective measures when detecting any breaches of applicable data protection rules

- Must have access to all data files and all data processing within the company as well as to all other information that he/she requires to fulfill his/her duties
- Must maintain records of all data files controlled by the company and provide this list to the FDPIC or affected data subjects upon request, and
- May not carry out any other activities that are incompatible with his/her duties as data protection officer

The data controller must notify the FDPIC of the appointment of a data protection officer and thereupon such data controller will be listed on the public list of companies exempt from the requirement to register their data files.

COLLECTION & PROCESSING

The following principles apply to the collection and processing of personal data (including data of legal entities):

- Personal data may only be processed lawfully, in good faith and according to the principle of proportionality.
- The collection of personal data and, in particular, the purpose of its processing must be evident to the data subject.
- Personal data should only be processed for a purpose that is indicated or agreed at the time of collection, evident from the circumstances at the time of collection, or provided for by law.
- The data controller and any processor must ensure that the data processed is accurate.
- Personal data must not be transferred abroad if the privacy of the data subject may be seriously endangered (see below).
- Personal data must be protected from unauthorized processing by appropriate technical and organizational measures.
- Personal data must not be processed against the explicit will of the data subject, unless this is justified by:
    - An overriding private or public interest, or
    - law, and
- Sensitive personal data or personality files must not be disclosed to a third party, unless this is justified by:
    - the consent of the data subject (which must be given expressly in addition to being voluntary and based on adequate information)
    - an overriding private or public interest, or
    - law

TRANSFER

Personal data may be transferred outside Switzerland if the destination country offers an adequate level of data protection. The FDPIC maintains and publishes a list of such countries. It should be noted that under Swiss data protection law, remote access to data residing in Switzerland from outside of Switzerland is considered as transfer / disclosure abroad.

The FDPIC deems the data protection legislation of all EU and EEA countries to be adequate with regard to personal data of individuals. With regard to personal data of legal entities, only a few EU or EEA countries, such as Austria and Liechtenstein, and Argentina (for legal entities domiciled in Argentina), are deemed to provide an adequate level of data protection.

In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if at least one of the following conditions if fulfilled:

- Sufficient safeguards, such as data transfer agreements, or other contractual clauses, ensure an adequate level of protection abroad. Data transfer agreements or other contractual clauses must be notified and submitted for approval to the FDPIC whereas mere information is sufficient if model clauses acknowledged by the FDPIC (such as the EU Standard Contractual Clauses for Controller-to-Controller or Controller-to-Processor Transfers, with the necessary amendments for Switzerland) are used.
- Since April 12, 2017, US companies that process data can be certified under the Swiss-US Privacy Shield regime and thereby make themselves subject to its rules. To do so, they must register on the Department of Commerce (DOC) website privacyshield.gov/PrivacyShield/ApplyNow and meet the certification requirements. Accordingly, the FDPIC has amended his list of countries indicating adequate data protection legislation, now listing the US among the countries with adequate legislation if the transferee is certified under the Swiss-US Privacy Shield. According to established practice by

the FDPIC, no notification is necessary in case the transferee is certified under the Swiss-US Privacy Shield. It should, however, be noted that certification under the EU-US Privacy Shield does by itself not entail certification for the Swiss-US Privacy Shield.

- Binding corporate rules that ensure an adequate level of data protection in cross-border data flows within a single legal entity or a group of affiliated companies. Such rules must be notified to the FDPIC.
- The data subject consents to the particular data export (consent must be given for each individual case or, according to legal doctrine and practice, for a number of cases under the same specific circumstances, *eg*, data export for certain specifically defined purposes; in contrast, a generic consent which does not further specify the circumstances under which data is disclosed is not sufficient).
- The processing is directly connected with the conclusion or performance of a contract with the data subject.
- The disclosure is essential in order to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal rights before the courts.
- The disclosure is required in order to protect the life or the physical integrity of the data subject, or the data subject has made the personal data publicly accessible and has not expressly prohibited its processing.

SECURITY

The data controller and any processor must take adequate technical and organizational measures to protect personal data against unauthorized processing and ensure its confidentiality, availability and integrity. In particular, personal data must be protected against the following risks:

- Unauthorized or accidental destruction
- Accidental loss
- Technical errors
- Forgery, theft or unlawful use
- Unauthorized altering, copying, accessing or other unauthorized processing

The technical and organizational measures must be appropriate, in particular with regard to the purposes of the data processing, the scope and manner of the data processing, the risks for the data subjects and the current technological standards. The ODP sets out these requirements in more detail.

BREACH NOTIFICATION

There is no explicit statutory requirement to notify the FDPIC or the affected data subjects of data security breaches under the DPA. However, depending on the scale and severity of a breach, a notification of the data subjects may be necessary based on the data controller's and processor's obligation to ensure data security (to avoid further damage), the principle of good faith or pursuant to contractual obligations.

ENFORCEMENT

The FDPIC does not have specific direct powers to enforce the DPA. He may investigate cases on his own initiative or at the request of a third party and may issue recommendations that a specific data processing practice be changed or abandoned. If the FDPIC's recommendation is not complied with, he may refer the matter to the Swiss Federal Administrative Court for a decision (as a recent example, in response to a health insurer's practice to collect health data from policyholders via a mobile app and in turn providing cash or other monetary value to these policy holders, the FDPIC has recommended to the health insurer in April 2018, inter alia, to withdraw the mobile app from the market. The health insurer refused to implement the FDPIC's recommendations and the FDPIC has subsequently referred the matter to the Swiss Federal Administrative Court for a decision).

Furthermore, the DPA provides for criminal liability and fines of up to CHF10,000 if a private person intentionally fails to comply with the following obligations under the DPA:

- Duty to provide information when collecting sensitive data and personality profiles
- Duty to safeguard the data subject's right to information
- Obligation to notify the FDPIC with regard to contractual clauses or binding corporate rules in connection with data

transfers abroad
- Obligation to register data files, or
- Duty to cooperate in an FDPIC investigation

Furthermore, the DPA provides for criminal liability and fines of up to CHF10,000 if a private person willfully discloses confidential, sensitive personal data or personality profiles that have come to his or her knowledge in the course of his or her professional activities, where such activities require the knowledge of such data, or in the course of his or her activities for a person bound by professional secrecy obligations or in the course of training with such a person.

Criminal proceedings must be initiated by the competent cantonal prosecution authority.

Finally, under Swiss civil law the data subject may apply for injunctive relief and may file a claim for damages as well as satisfaction and/or surrender of profits based on the infringement of his/her privacy.

ELECTRONIC MARKETING

Electronic marketing practices must comply with the provisions of the Swiss Federal Act against Unfair Competition (UCA).

With regard to the sending of unsolicited automated mass advertisement (which, in addition to emails, includes SMS, automated calls and fax message(s)), the UCA generally requires prior consent by the recipient, *ie*, 'opt-in'. As an exception, mass advertisings may be sent without the consent of the recipient:

- If the sender received the contact information in the course of a sale of his / her products or services
- If the recipient was given the opportunity to refuse the use of his / her contact information upon collection (opt-out), and
- If the mass advertising relates to similar products or services of the sender

In addition, mass advertising emails must contain the sender's correct name, address and email contact and must provide for an easy-access and free of charge 'opt-out' from receiving future advertisements.

The UCA generally applies to business-consumer relationships as well as to business-business relationships, *ie*, mass advertisements sent to individuals and to corporations are subject to the same rules.

Direct marketing by telephone is lawful in Switzerland as long as it is not done in an aggressive way (*eg*, by repeatedly calling the same person). However, the UCA prohibits direct marketing by telephone to people who do not wish to receive commercial communication and have expressed that wish (*ie*, opted-out) by having their entry marked in the telephone books and online telephone registers (*eg*, through an asterisk next to their name).

In addition to the rules of the UCA, the general data protection principles under the DPA also apply with regard to electronic marketing activities, *eg*, the collection and maintenance of email addresses or processing of any other personal data.

ONLINE PRIVACY

The processing of personal data in the context of online services is subject to the general rules pertaining to the collection of personal data under the DPA. In addition, certain aspects of online privacy are covered by other regulations, such as the use of cookies which is also subject to the Swiss Telecommunications Act (TCA).

Under the TCA, the use of cookies is considered to be processing of data on external equipment, *eg*, another person's computer. Such processing is only permitted if users are informed about the processing and its purpose as well as about the means to refuse the processing, *eg*, by configuring their web browser to reject cookies.

In addition, the general rules under the DPA apply where cookies collect data related to persons who are identified or identifiable, *ie*, personal data. The collection of personal data through cookies as well as the purpose of such a collection must be evident to the data subject. The personal data collected may only be processed for the purpose:

- Indicated at the time of collection
- That is evident from the circumstances, or

- That is provided for by law

Where the personal data collected through a cookie is:

- Considered sensitive data, *eg*, data regarding religious, ideological, political views or activities, or
- So comprehensive that it forms a personality profile, *ie*, permits an assessment of essential characteristics of the personality of a person

The stricter rules pertaining to the processing of sensitive personal data are applicable.

These stricter rules provide, inter alia, that the data subject must be informed of:

- The identity of the data controller
- The purpose of data processing, and
- The categories of data recipients if the data shall be disclosed to third parties.

Further, in relation to the processing of sensitive personal data implied consent is not sufficient; consent must be given expressly.

KEY CONTACTS

Schellenberg Wittmer Ltd
www.swlegal.ch/

Roland Mathys
Partner / Attorney at Law
T +41 (0)44 215 3662
roland.mathys@swlegal.ch

Christine Beusch-Liggenstorfer
Of Counsel/Attorney at Law
T +41 (0)44 215 5272
christine.beusch@swlegal.ch

Samuel Klaus
Associate / Attorney at Law
T +41 (0)44 215 3695
samuel.klaus@swlegal.ch

Claudia Jung
Associate / Attorney at Law
T +41 (0)44 215 3498
claudia.jung@swlegal.ch

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

TAIWAN

Last modified 28 January 2019

LAW

The former Computer Processed Personal Data Protection Law (CPPL) was renamed as the Personal Data Protection Law (PDPL) and amended on May 26, 2010. The PDPL became effective on October 1, 2012, except that the provisions relating to sensitive personal data and the notification obligation for personal data indirectly collected before the effectiveness of the PDPL remained ineffective. The government later proposed further amendment to these and other provisions, which passed legislative procedure and became effective on March 15, 2016.

DEFINITIONS

Definition of personal data

According to PDPL, personal data means:

- Name
- Date of birth
- ID card number
- Passport number
- Characteristics
- Fingerprints
- Marital status
- Family
- Education
- Occupation
- Medical record
- Medical treatment
- Genetic information
- Sexual life
- Health checks
- Criminal records
- Contact information
- Financial conditions
- Social activities
- Other information which may directly or indirectly be used to identify a living natural person

Definition of sensitive personal data

According to the PDPL, sensitive personal data means the personal data relating to medical records, medical treatments, genetic information, sex life, health checks and criminal records.

NATIONAL DATA PROTECTION AUTHORITY

In Taiwan, there is no single national data protection authority. The various ministries and city / county governments serve as the competent authorities.

REGISTRATION

Unlike the CPPL, there is no need to register with any authorities for the collection, processing, usage and international transfer of personal data under the PDPL.

DATA PROTECTION OFFICERS

There is no requirement in Taiwan for the data controller to appoint a data protection officer. However, if the data controller is a government agency, a specific person should be appointed to be in charge of the security maintenance measures.

COLLECTION & PROCESSING

Under the PDPL, the data controller should not collect or process personal data unless there is specific purpose and should comply with one of the following conditions:

- Where collection / processing is explicitly stipulated by law
- Where there is a contract or quasi contract between the data controller and the data subject and there is proper security measures in place
- Where the data subject has him/herself disclosed such data to the public or where the data has been publicized legally
- Where it is necessary for public interest on statistics or the purpose of academic research conducted by a research institution. The data may not lead to the identification of a certain person after the treatment of the provider or by the disclosure of the collector
- Where consent has been given by the data subject (which may be assumed under certain circumstances where the data controller has explicitly informed the data subject of the information required by the PDPL, and the data subject has provided his/her personal data and has not expressed his / her rejection. Even so, the data controller has the burden of proof to show valid consent)
- Where it is necessary to enhance the public interest
- Where the personal data is obtained from publicly available sources, except that where the vital interest of the data subject requires more protection and the prohibition of the processing or usage of such personal information
- Where there is no infringement on the rights of interests of the data subject

Except for the exemptions stipulated in the PDPL (eg, if it is explicitly stipulated by law that the provision of such information is not required, or if the data subject is fully aware of the contents of the notice, or if it is not profit-seeking purpose and it is obviously not detrimental to the data subject), the data controller is permitted to collect and process personal data only if the data controller unambiguously informs the data subject of the following information prior to or upon the collection:

- Data controller's name
- Purpose(s) for collecting personal data
- Categories of personal data
- Period, area, recipients and means of using the data
- The data subject's rights and the methods by which the data subject may exercise those rights in accordance with the PDPL, and
- Where the data subject has the right to choose whether or not to provide the data, the consequences of not providing the data

The information collected should in principle only be used for the purpose notified and not for any other purpose unless falling within any of the exceptional circumstances as set forth in the PDPL (*eg*, where consent has been given by the data subject, or where it is beneficial to the rights or interests of the data subject).

In addition, the Employment Service Act and its Enforcement Rules require that an employer shall not request a job seeker or an employee to provide his / her privacy information which is unrelated to his/her employment. Such privacy information includes physiological information, psychological information and personal life information. When an employer asks a job seeker or an employee to provide his / her privacy information, the personal interest of the data subject should be respected; the request should not exceed necessary scope of specific purposes based on economic demand or public interest, and should have just and reasonable connection with the specific purposes.

As to sensitive personal data, its collection, processing or usage (including international transfer) is prohibited unless any of the statutory conditions is met, which include the circumstances where written consent of the data subject has been obtained (except that it exceeds the necessary scope of specific purposes, or other laws otherwise provide for, or the consent is contrary to his / her free will), or where the data subject has him / herself disclosed such data to the public or the data has been publicized legally.

TRANSFER

The central competent authority may restrict the international transfer of personal data by the data controller which is not a government agency in the following circumstances:

- Where it involves major national interests
- Where an international treaty or agreement specifies otherwise
- Where the country receiving personal data lacks proper regulations that protect personal data and that might harm the rights and interests of the data subject
- Where the international transfer of personal data is made to a third country through an indirect method in order to evade the provisions of the PDPL

SECURITY

Data controllers should adopt proper security measures (both technical and organizational) to prevent personal data from being stolen, altered, damaged, destroyed or disclosed.

The central competent authority may request the data controller which is a non-government agency to set up a plan for the security measures of the personal data file or the disposal measures for the personal data after termination of business.

BREACH NOTIFICATION

Where the personal data is stolen, disclosed, altered or infringed in other ways due to the violation of the PDPL, the data controller should notify the data subject after due inquiry.

ENFORCEMENT

Under the PDPL, the competent authority may perform an inspection, if it is necessary for the examination of the security measures of data files, of the disposal measures after termination of business, the limitation of international transfer, or other routine business, or if the PDPL may be violated. Those who perform the inspection may ask the data controller to provide a necessary explanation, take cooperative measures, or provide relevant evidence.

When the competent authority conducts such an inspection, it may seize or duplicate the personal data and files that may be confiscated or may be used as evidence. The owner, holder or keeper of the data or files should surrender them upon request.

In addition, a breach of the PDPL may be subject to criminal sanctions (if for a profit-seeking purpose), administrative fines, and civil compensation (collective action is permitted).

ELECTRONIC MARKETING

The PDPL applies to electronic marketing in the same way as to other marketing. Within the necessary scope of specific purposes of data collection, the data controller may use personal data for marketing. However, when the data subject refuses the marketing (a right to 'opt out'), the data controller should cease using such personal data for marketing. In addition, when making the first

marketing, the data controller should bear the costs to provide the data subject with the means to refuse marketing.

ONLINE PRIVACY

There is no special law or regulation applicable to online privacy. The PDPL applies to online and physical world in the same manner. As a result, online unique issues are not specifically addressed.

KEY CONTACTS

Formosa Transnational Attorneys at Law
www.taiwanlaw.com/

Chun-yih Cheng
Senior Partner
Formosa Transnational Attorneys at Law
T +886 2 27557366 Ext 158
chun-yih.cheng@taiwanlaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

TAJIKISTAN

Last modified 27 January 2019

LAW

- Personal Data Protection Law, No.1537 of 3 August 2018
- Protection Data Law, No.631 of 15 May 2002
- Informatization Law, No. 40 of 6 August 2001
- Information Law, No.609 of 10 May, 2002
- Regulation on Certification of Information Security Facilities, Attestation of Information Objects and the Procedure for Their State Registration, No.404 of 1 October 2004
- The List of Information Security Facilities Subject to State Certification, No.424 of 24 February 2008

DEFINITIONS

Personal Data Protection Law (hereinafter '**PDPL**') identifies personal data as any information about the facts, events and circumstances of the life of a data subject, which allow to identify him/her.

Under the foregoing law the data subject is considered a physical person, to whom relevant personal data refers.

PDPL does not define the term of sensitive data. However it provides the definition of biometric personal data which includes biometrical and physiological data which identifies the data subject. Biometric personal data may be collected upon receipt of the subject's consent.

NATIONAL DATA PROTECTION AUTHORITY

The Main Department for the Protection of State Secrets under the Government of the Republic of Tajikistan (hereafter 'Regulator').

Address:
F.Niyozi 37
Dushanbe, Tajikistan
734001

Tel: +(992 37) 2-27-86-17
info@ggs.tj
Website

REGISTRATION

Under PDPL pre-notification of the Regulator while collecting, processing or maintaining a database consisting of personal data is not required.

However, Data Protection Law requires to certify all information security facilities (including cryptographic, software, organizational, technical and hardware-based), as well as foreign made facilities designated for the protection of information.

The list of information protection facilities is set forth by the Main Department for the Protection of State Secrets under the Government of the Republic of Tajikistan (Regulator). Certification is carried out on the basis of an agreement concluded between Regulator and data controller.

DATA PROTECTION OFFICERS

Tajik law does not require to appoint any Data Protection Officer or any similar positions.

COLLECTION & PROCESSING

PDPL provides the following definitions of collection and processing of personal data:

- Collection of personal data is an action aimed at receiving personal data
- Processing of personal data are actions aimed at:
    - Recording
    - Systemization
    - Storage
    - Amendment
    - Replenishment
    - Extraction
    - Usage
    - Spread
    - Impersonation
    - Blocking, and
    - Destruction of personal data

Collection and processing of personal data is allowed when the following conditions are met:

- The data subject's consent or that of his / her legal representatives
- The processed and collected information is in compliance with the lawful aims of the data controller
- The processed and collected information is accurate and complete
- The data subject has access to the processed and collected data relating to him / her and has the right to require rectification of the relevant information
- The data collector has duly certified all the relevant equipments and facilities designated for processing and collection of data with the Regulator

Article 11 of the PDPL entitles the data collector to process personal data without receiving the data subject's consent, if it is necessary for governmental authorities to carry out their functions or for the purpose of protecting the constitution rights and freedom of the citizens.

TRANSFER

Transfer of personal data is allowed if the rights and freedom of the data subject are not violated. With regard to cross-border transfers of personal data the PDPL does not impose any restrictions on the data controller if the foreign country provides adequate protection of personal data.

Where there is no adequate protection of personal data, a cross border transfer is permitted in the following cases:

- The data subject's consent is obtained
- The transfer is provided pursuant to an international treaty recognized by Tajikistan, or
- The transfer is necessary for the purpose of protecting citizens rights and freedom, health and morality and public order of the state

SECURITY

The data controller is obliged to take appropriate measures against unauthorized processing, accidental loss, or modification of personal data.

BREACH NOTIFICATION

Currently, there is no formal requirement in Tajikistan to report data breaches to any authority or data subject.

ENFORCEMENT

Enforcement of Data Protection Law ('DPL') is primary done by the Main Department for the Protection of State Secrets under the government of Tajikistan.

In addition, Tajikistan courts, the Prosecutor's Office, the Ministry of Internal Affairs and other law enforcement bodies have the authority to ensure compliance and enforce the provisions of DPL within their competence.

Violations of DPL may result in civil, administrative and criminal sanctions, including:

- Administrative fines up to approximately 1750 US$
- Imprisonment of up to 10 years, and
- The right to claim compensation of damages, including emotional distress under civil proceedings

ELECTRONIC MARKETING

Currently, there is no law or regulation in Tajikistan that specifically regulates electronic marketing.

ONLINE PRIVACY

Currently, there is no law or regulation in Tajikistan that specifically regulates online privacy.

KEY CONTACTS

Alisher Hoshimov
Senior Associate
Centil Law Firm
T +992900878833
alisher.k@centil.law

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

THAILAND

Last modified 31 May 2019

LAW

The Personal Data Protection Act 2019 (PDPA) of Thailand was published in the Government Gazette on 27 May 2019. The Act will be effective from the day after publication, which is 28 May 2019.

DEFINITIONS

"Committee" means the Personal Information Protection Committee.

"Personal Data" means any data pertaining to a person that enables the identification of that person, whether directly or indirectly, but specifically excluding data of the deceased.

"Personal Data Administrator" means a person or corporate entity who has a decisive power on compiling, using or disclosing Personal Data (the "*Data Administrator*").

"Personal Data Processor" means a person or corporate entity who carries out the collecting, applying, or disclosing of personal data according to the instruction or on behalf of the **Personal Data Administrator**. Such Personal Data Processor shall not be the same person as the Personal Data Administrator (the "*Data Processor*").

"Person" means a natural person.

NATIONAL DATA PROTECTION AUTHORITY

The Ministry of Digital Economy and Society.

REGISTRATION

No details yet for this country.

DATA PROTECTION OFFICERS

The Personal Information Protection Committee and the data protection officials working under the supervision of said commission.

COLLECTION & PROCESSING

The collection of personal information may be done as necessary under the lawful means and purposes. A *Data Administrator* may collect, process, use or disclose Personal Data of a Person only when prior affirmative consent has been given by the data subject. The consent can be given in writing or through electronic means.

The *Data Administrator* shall only obtain the data directly from the data subject.

The *Data Administrator* must inform the data subject of the purpose of collecting the data, what data is to be collected, and to whom the data will be disclosed.

Additionally, the request for consent must be clearly separated from other messages. The message must be delivered in a format which is easily accessible and understandable, using language that is easy to understand. The message should not be misleading or cause data subjects to misunderstand the purpose of collecting the data. The Commission may require the *Data Administrator* to request consent from the data subject in accordance with any announcement that the board may make from time to time.

The Thailand PDPA does not provide a specific definition of "*sensitive data.*" However, according to the PDPA, it is prohibited to collect information related to ethnicity, political opinions, religious beliefs, sexual orientation, criminal history, health information, disability, trade union information, genetic data, biological data or any other information that affects the data subject in the same way, unless there are specific laws which stipulate otherwise, e.g. for the protection of health or physical condition of the data subject.

The PDPA does allow, in some limited circumstances, for an exemption to the requirement to obtain consent from the data subject where the data is collected from another Person who is not the data subject.

In obtaining consent from the owner of the Personal Data, the *Data Administrator* must take into account the absolute independence of the owner of the personal information in giving the consent. In entering into a contract, including to provide any services, there must not be any condition for consent to be granted to collect, use or disclose personal information that is not necessary or relevant to entering into such contract or services.

Parental consent for minors

Parental consent is required in cases where minors may not provide the consent themselves. Where the data subject is under 10 years old, parental consent is required from the parent who is authorized to act on behalf of the minor, as stipulated in law.

In cases where the data subject lacks the relevant capacity, the consent must be obtained by the guardian/custodian of such data subject.

Rights of the data owners

Data owners are entitled to request access to personal data pertaining to them except in cases where, among others, the request is not under the provisions of applicable laws or court orders.

Data owners are also entitled to request that their personal data be destroyed, temporarily suspended, or maintained anonymized.

Data protection

Data administrators are required to implement proper and adequate procedures to keep personal data secure. The committee may, from time to time, issue guidelines that Data Administrators can use as a reference for their data protection practices. The Committee may also implement specific requirements on the qualification of Data Administrators and Data Processors.

TRANSFER

The PDPA prohibits the transfer of personal data to third countries where data protection regulations are substantially deficient, except when the transfer is carried out according to one of the following scenarios:

- where the transfer is processed according to the laws;
- where the transfer is carried out after obtaining the specific consent from the data owner, who has been made aware of the third country's insufficient data protection laws;
- where the transfer is carried out according to the obligations of a contract to which the data owner is a party that has an obligation to perform;
- where the transfer of data to a third country is conducted in order to prevent or suspend harm to the life, body or

health of the owner of the personal information or other persons, while the data owner lacks the capacity to give consent; and

- when it is necessary, for the purpose of carrying out the transfer for significant public benefit.

SECURITY

No details yet for this country.

BREACH NOTIFICATION

No details yet for this country.

ENFORCEMENT

The owner of the personal information may file a complaint to the Committee in in the event that the *Data Administrators* or *Data Processors*, including their employees, violate or fail to comply with the PDPA or announcement issued under the Act. The Committee shall assign a proficient sub-committee to investigate and verify each of the issues submitted to the Committee's office.

Where the sub-committee considers or verifies that complaints or actions may be amenable and the parties wish to mediate such issues, the sub-committee will conduct mediation. If the complaint or action cannot be reconciled or mediated or, if the mediation occurs but is not successful, the sub-committee has the right to issue one of the following orders:

- to instruct the *Data Administrator* or *Data Processor* to act or correct their actions within the specified period; or
- to instruct the *Data Administrator* or *Data Processor* to refrain from taking any actions that cause damage to the data owners as well as to act in any appropriate manner to prevent any further damage to the data owner, within a certain period of time.

In the event that the *Data Administrator* or *Data Processor* refuses to follow the administrative order, the authority may apply enforcement provisions, which may include seizing of properties or freezing of business activities under the law related to administrative duties.

ELECTRONIC MARKETING

No details yet for this country.

ONLINE PRIVACY

No details yet for this country.

KEY CONTACTS

Peter Shelford
Country Managing Partner, Thailand
T +662 686 8533
peter.shelford@dlapiper.com

Chadaporn Ruangtoowagoon
Senior Associate
T +662 686 8579
chadaporn.ruangtoowagoon@dlapiper.com

Robert Tang
Senior Consultant
T +662 686 8551
robert.tang@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

TRINIDAD AND TOBAGO

Last modified 28 January 2019

LAW

The Data Protection Act, 2011 (DPA) provides for the protection of personal privacy and information processed and collected by public bodies and private organizations.

The DPA was partially enacted on January 6, 2012 by Legal Notice 2 of 2012, and only Part I and sections 7 to 18, 22, 23, 25(1), 26 and 28 of Part II have come into operation.

No timetable has been set for enacting the remainder of the DPA, and it is possible that there may be changes to the remainder of the legislation before it is proclaimed.

DEFINITIONS

Definition of personal data

Personal information is defined as information about an identifiable individual that is recorded in any form including:

- The name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual
- The address and telephone number of the individual
- Any identifying number, symbol or other particular identifier designed to identify the individual
- Information relating to the individual's race, nationality or ethnic origin, religion, age or marital status
- Information relating to the education or the medical, criminal or employment history of the individual, or information relating to the financial transactions in which the individual has been involved or which refer to the individual
- Correspondence sent to an establishment by the individual
- Information that is explicitly or implicitly of a private or confidential nature, and any replies to such correspondence that would reveal the contents of the original correspondence
- The views and opinions of any other person about the individual
- The fingerprints, DNA, blood type or other biometric characteristics of the individual

Definition of sensitive personal data

Sensitive personal information is defined as personal information on a person's:

- Racial or ethnic origins
- Political affiliations or trade union membership
- Religious beliefs or other beliefs of a similar nature
- Physical or mental health or condition
- Sexual orientation or sexual life

- Criminal or financial record

NATIONAL DATA PROTECTION AUTHORITY

The Office of the Information Commissioner is responsible for the oversight, interpretation and enforcement of the DPA. It has broad authority, including to authorize the collection of personal information about an individual from third parties and to publish guidelines regarding compliance with the Act.

REGISTRATION

There is no registration requirement under the DPA.

DATA PROTECTION OFFICERS

There is no such requirement under the DPA.

COLLECTION & PROCESSING

The knowledge and consent of the individual is required for the collection, use and disclosure of personal information. Collection must be made in accordance with the purpose identified by the organization collecting the personal information.

Sensitive personal information may not be processed except as specifically permitted by law.

The DPA includes provisions that relate specifically to the collection and processing of personal information by public bodies and private enterprises, however, these are not yet in force. Nevertheless, they are presented below.

Public Bodies

Part III of the DPA provides that a public body may collect and process personal data when the following conditions are met: the collection of that information is expressly authorized by law and

- The information is collected for the purpose of law enforcement
- The information relates directly to and is necessary for an operating program or activity of the public body when the collection of personal information is collected directly from the individual:
    - Another method of collection is authorized by the individual, Information Commissioner or law
    - The information is necessary for medical treatment
    - The information is required for determining the suitability of an award
    - The information is collected for judicial proceedings
    - The information is required for the collection of a debt or fine, or
    - It is required for law enforcement purposes
- The individual is informed of the purpose for collecting his / her personal information; the legal authorization for collecting it and contact details of the official or employee of the public body who can answer the individual's questions about the collection

Private Bodies

Part IV of the DPA provides that the collection and processing of personal information by private organizations must be in accordance with certain Codes of Conduct (which are to be determined by the Office of the Information Commissioner in consultation with the private sector) and the General Privacy Principles (which are currently in force).

Sensitive Information

Sensitive personal information may not be processed by public bodies and private organizations without the consent of the individual unless:

- It is necessary for the healthcare of the individual

- The individual has made the information public
- It is for research or statistical analysis
- It is by law enforcement
- It is for the purpose of determining access to social services, or
- As otherwise authorized by law

TRANSFER

Section 6(1) of the DPA provides that personal information may be transferred outside of Trinidad and Tobago only if the foreign country requesting the individual's personal information has safeguards comparable to Trinidad and Tobago's for the regulation of the personal information which are.

In this regard, the Office of the Information Commissioner is required to publish a list of countries which have comparable safeguards for personal information as provided by this Act in the Gazette and in at least two newspapers in daily circulation in Trinidad and Tobago. As of April 4, 2018, such publication has not happened.

Sections 72(1) and (2) of the DPA (neither of which are in force as yet) provide that where a mandatory code is developed for private bodies, at a minimum, it must require that personal information under the custody or control of a private organization not be disclosed to a third party without the consent of the individual to whom it relates, subject to certain conditions. Where personal information under the custody and control of an organization is to be disclosed to a party residing in another jurisdiction, the organization must inform the individual to whom the information relates.

Section 6 of the DPA, which is in force, states that all persons who handle, store or process personal information belonging to another person are subject to the following General Privacy Principles:

- An organization shall be responsible for the personal information under its control.
- The purpose for which personal information is collected shall be identified by the organization before or at the time of collection.
- Knowledge and consent of the individual are required for the collection, use or disclosure of personal information.
- Collection of personal information shall be legally undertaken and be limited to what is necessary in accordance with the purpose identified by the organization.
- Personal information shall only be retained for as long as is necessary for the purpose collected and shall not be disclosed for purposes other than the purpose of collection without the prior consent of the individual.
- Personal information shall be accurate, complete and current, as is necessary for the purpose of collection.
- Personal information is to be protected by such appropriate safeguards according to the sensitivity of the information.
- Sensitive personal information is protected from processing except where specifically permitted by written law.
- Organizations are to make available documents regarding their policies and practices related to the management of personal information to individuals, except where otherwise provided by written law.
- Organizations shall, at the request of the individual, disclose all documents relating to the existence, use and disclosure of personal information, such that the individual can challenge the accuracy and completeness of the information, except where otherwise provided by written law.
- The individual has the ability to challenge the organization’s compliance with the above principles and receive timely and appropriate engagement from the organization.
- Personal information which is requested to be disclosed outside of Trinidad and Tobago shall be regulated and comparable safeguards to those under this Act shall exist in the jurisdiction receiving the personal information.

SECURITY

The DPA generally requires that personal information is protected by appropriate safeguards based on the sensitivity of the information. Sensitive personal information may not be processed except where permitted by law.

BREACH NOTIFICATION

There is no provision in the DPA for notifying data subjects or the Information Commissioner of a security breach.

ENFORCEMENT

The Office of the Information Commissioner is responsible for monitoring the administration of this Act to ensure that its purposes are achieved.

The Information Commissioner has several broad powers to conduct audits and investigations of compliance with the DPA.

Part V of the DPA (which is not in force) details the penalties for contraventions of the DPA and also makes further provisions for the enforcement of the DPA.

ELECTRONIC MARKETING

The DPA has no specific provision regarding electronic marketing.

However, Section 58 of the Electronics Transaction Act (not yet in force) requires that anyone performing the following acts shall provide the consumer with a clearly specified and easily activated option to opt out of receiving future communications:

- Sending unsolicited commercial communications through electronic media to consumers in Trinidad and Tobago
- Knowingly using an intermediary or a telecommunications service provider in Trinidad and Tobago to send unsolicited commercial communications
- Sending unsolicited electronic correspondence to consumers while having a place of business in Trinidad and Tobago

ONLINE PRIVACY

The DPA has no specific provision regarding online privacy.

KEY CONTACTS

M. Hamel Smith & Co.
www.trinidadlaw.com/

Jonathan Walker
Partner
T +1 868 821 5500 ext. 5625
jonathan@trinidadlaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

TUNISIA

Last modified 28 January 2019

LAW

Law n° 2004-63 dated July 27, 2004, on the Protection of Personal Data, regulates personal data, but even before that, Tunisia was already a pioneer in its region since 2002 in the field of personal data protection. This law was endorsed by the 2014 constitutional embodiment of the protection of privacy, which has placed this protection at the forefront of the rights and freedoms to be guaranteed in the new Republic.

Additionally, articles 56, 61 and 75 of the Organic Law n° 2015-26 of August 7, 2015 on the Fight Against Terrorism and the Prohibition of Money Laundering addresses the subject of personal data and when the use of personal data is permitted.

Tunisia became the 51st Member State of the Council of Europe Convention 108 on November 1, 2017.

In March 2018, it introduced a new draft law on the protection of personal data in line with the new European GDPR in Parliament.

DEFINITIONS

Definition of personal data

Article 4 of Act n° 2004-63 of July 27, 2004 defined personal data as all information regardless of their origin or form and which directly or indirectly allows to identify or make identifiable a natural person, with the exception of information related to public life or considered as such by law.

Definition of sensitive personal data

Act n° 2004-63 of July 27, 2004 did not give a clear definition of sensitive personal data, but it listed some personal data the processing of which is either prohibited, or would question the data subject's prior consent or the national authority's authorization.

The processing of personal data is prohibited when involving criminal history and proceedings, criminal prosecution, penalties, preventative measures or judicial history.

In addition, the processing of personal data which directly or indirectly concerns the following is also prohibited:

- Racial or genetic origins
- Religious beliefs
- Political opinions
- Philosophical or union activism, or
- Health and scientific research

NATIONAL DATA PROTECTION AUTHORITY

The National Authority for Protection of Personal Data (the Instance) was created by Decree n° 2007-3003 of November 27th, 2007.

REGISTRATION

Any processing of personal data shall be subject to a prior declaration filed at the headquarters of the National Authority for Protection of Personal Data, or by any other means leaving a written record.

- The declaration shall be made by the controller or his legal representative.
- The declaration does not exempt third parties from liability.
- The conditions and procedures for submitting the declaration shall be laid down by decree.
- The Commission may object to the processing of personal data within one month from when the declaration is accepted. (Article 7 of the 2004 Act).

DATA PROTECTION OFFICERS

Under Tunisian law, there is no reference to Data Protection Officers.

COLLECTION & PROCESSING

The following principles generally apply to the processing of personal data:

- Personal data must be collected directly from the data subject.
- Personal data collected from third parties are permitted whenever the data subject, his heirs or his agent have provided their consent.
- The processing of personal data must respect human dignity, privacy and public liberties.
- The collecting of personal data shall be exclusively carried out for lawful and clear purposes.

Among the main prerequisites for the legitimate processing of personal data is the informed consent of the data subject, which means that the processing of personal data cannot be carried out without the express and written consent of the data subject. This consent shall be governed by the general rules of law if the data subject is incompetent or unauthorized or incompetent to sign.

The data subject or his agent is allowed to withdraw his consent, at any time during the processing.

Additionally, and in the spirit of child protection, Tunisian law has provided extra protection to personal data relating to children as this kind of data cannot be carried out without the consent of the child's agent and after authorization of the juvenile and family court judge.

Finally, the consent provided for the processing of personal data under a specific given shall not apply to other forms or purposes.

TRANSFER

The transfer of personal data is treated in the 5th Chapter of the 2004 Act on the protection of personal data (Articles 47 to 52), and is generally prohibited or subject to strict measures, including prior authorization (submitted to the National Authority for Protection of Personal Data), and the explicit consent of the person in question, which is mandatory. The transfer of personal data to a foreign country is prohibited whenever it may endanger public security or Tunisia's vital interests.

The international transfer of personal data may not take occur if the foreign country does not provide an adequate level of protection. In every case, the authorization of the Instance is required before the transfer of personal data. The Instance shall issue its decision within one month from the date of receipt of the application.

SECURITY

The National Authority for Protection of Personal Data is responsible for determining the proper measures and necessary safeguards in order to protect personal data.

BREACH NOTIFICATION

Under Tunisian Law, it is up to the person in question to make this kind of notification, or to its heirs and agents in certain circumstances.

Mandatory breach notification

The public prosecutor in the jurisdiction where the investigation takes place shall be informed by The National Authority for Protection of Personal Data of any offenses that it has detected.

ENFORCEMENT

The National Authority for Protection of Personal Data is legally mandated to ensure compliance with the provisions of the Law, but there is no information about cases where sanctions were applied to personal data infringements.

A draft bill on personal data is currently being considered by the Parliamentary Committee on Rights and Freedoms in the Tunisian Parliament, which revolutionizes the existing Law, and when adopted, will be in correspond to the European standards for Data Protection.

ELECTRONIC MARKETING

Electronic Marketing is regulated under Tunisian Law by The Electronic Exchanges and Electronic Commerce Law n° 2000-83 enacted on August 9, 2000.

This law is quite comprehensive and regulates the main aspects of this field. For instance:

- The preservation of the electronic document is as important as the preservation of the written document
- Each person using an electronic signature device shall:
    - Take minimum precautions to avoid illegitimate use of encryption elements or personal signature equipment
    - Inform the electronic certification service provider of any fraudulent use of his electronic signature

ONLINE PRIVACY

There is no specific mention to online privacy under the 2004 law on the Protection of Personal Data.

However, the same safeguards including restrictions and sanctions apply as well to online privacy under Tunisian Law.

Furthermore, it is prohibited to use the processing of personal data for promotional purposes unless the data subject, his heirs or his tutor gives his explicit and specific consent.

KEY CONTACTS

Mohamed Lotfi El Ajeri
Managing Partner
Al Ajeri Lawyers
T +(216) 71 288 251 – 71 287 238
mlelajeri@eal.tn

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

TURKEY

Last modified 28 January 2019

LAW

The main piece of legislation covering data protection in Turkey is the Law on the Protection of Personal Data No. 6698 dated April 7, 2016 (LPPD). The LPPD is primarily based on EU Directive 95/46/EC.

To date, the legislature has enacted several regulations to implement various aspects of the LPPD. The notable ones are mentioned below:

- Regulation on the Erasure, Destruction and Anonymizing of Personal Data (published in the Official Gazette dated October 28, 2017, numbered 30224)
- Regulation on the Working Procedures and Principles of Personal Data Protection Board (published in the Official Gazette dated November 16, 2017, numbered 30242)
- Regulation on the Registry of Data Controllers (published in the Official Gazette dated December 30, 2017, numbered 30286)
- Regulation on the Organization of Personal Data Protection Authority (published in the Official Gazette dated April 26, 2018, numbered 30403)
- The Communiqué on Procedures and Principles for Compliance with the Obligation to Inform (published in the Official Gazette dated March 10, 2018, numbered 30356)
- The Decision of Data Protection Board, dated January 31, 2018, numbered 2018/10 on Adequate Measures to be taken by Data Controllers in Processing the Special Categories of Personal Data

Certain general laws such as the Turkish Criminal Code no. 5237 and sector specific laws such as Electronic Communications Law No. 5809 also touch upon data protection and are mentioned below when relevant.

DEFINITIONS

Definition of personal data

In the LLPD, personal data is defined as "Any information relating to an identified or identifiable natural person."

Definition of sensitive personal data

Sensitive personal data (Special Categories of Personal Data under the LPPD) is defined as "personal data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, clothing, membership of associations, foundations or trade unions, information related to health, sex life, previous criminal convictions and security measures, and biometric and genetic data."

NATIONAL DATA PROTECTION AUTHORITY

The national data protection authority is the *Kiisel Verileri Koruma Kurumu* (Personal Data Protection Authority). The Personal Data Protection Authority's decision-making body is *Kiisel Verileri Koruma Kurulu* (Personal Data Protection Board). The organizational structure of the Authority and the duties and powers of its bodies are regulated under the Regulation on the Organization of Personal Data Protection Authority and the Regulation on the Working Procedures and Principles of Personal Data Protection Board.

Kiisel Verileri Koruma Kurumu

Nasuh Akar Mah. Ziyabey Cad. 1407. Sok. No: 4

06520 Balgat-Çankaya/Ankara

T +90 312 216 5050

http://www.kvkk.gov.tr

REGISTRATION

Pursuant to the LPPD and the Regulation on the Registry of Data Controllers, data controllers are required to enroll in the Registry of Data Controllers before proceeding with data processing.

The Regulation on the Registry of Data Controllers was published in the Official Gazette dated December 30, 2017, and entered into force on January 1, 2018. It regulates the establishment of a publicly accessible registry, which is to be held by the Personal Data Protection Authority and the procedures and principles concerning enrollment in the registry.

Under this Regulation, all data controllers are required to enroll in the Registry of Data Controllers before proceeding with data processing. However, the Personal Data Protection Board may bring an exception to the obligation of enrollment by taking into account the nature and number of personal data, purpose of processing personal data, and other objective criteria. Data controllers are not required to enroll in the Registry of Data Controllers in the following circumstances:

- The processing of personal data is required for criminal investigation or for prevention of a criminal offense
- If the personal data being processed is already publicized by the data subject
- If, based on the authority given by Law, personal data processing is required for disciplinary investigation or prosecution and execution of the supervision or regulation duties to be conducted by public institutions and organizations and professional organizations with public institution status or
- If processing of personal data is required to protect the economic and financial interests of the State in relation to budget, tax and financial matters

Over the past year, the Personal Data Protection Board has enumerated additional exceptions to enrollment obligation:

- Data controllers who process personal data by non-automatic means as a part of a filing system, lawyers, independent accountants and financial advisors
- Natural or legal persons having less than 50 employees per annum and annual balance less than 25 million Liras and whose main field of activity is not processing special categories of personal data.

Data controllers who are non-resident in Turkey shall enroll in the registry through a representative they assign in Turkey. Legal persons in Turkey or Turkish citizens may be assigned as representatives for this purpose.

In addition, both legal entities resident in Turkey and the above-mentioned representatives of non-resident data controllers shall, as part of the enrollment procedure, appoint an individual to act as "contact person" for both the Personal Data Protection Authority and for data subjects.

Operations related to the Registry of Data Controllers shall be carried out through VERBIS (Data Controllers Registry Information System) by data controllers. The Personal Data Protection Authority, with its decision dated July 19, 2018, numbered 2018/88, sets forth the dates for the registration through VERBIS for four categories of data controllers.

Data Controllers	Commencement Date of Registration	Due Date
Any data controller who has more than 50 employees or whose total annual balance is more than TL 25,000,000	October 1, 2018	September 30, 2019
Non-resident individual and legal entity data controllers	October 1, 2018	September 30, 2019
Any data controller who has less than 50 employees and whose total annual balance is less than TL 25,000,000, but who process sensitive personal data as their main activity	January 1, 2019	March 31, 2020
Public institutions and organizations	April 1, 2019	June 30, 2020

Administrative fines of between ₺20,000 (approx. €3,250) and ₺1 million (approx. €162,000) may be imposed on data controllers breaching obligations regarding the Registry of Data Controllers.

DATA PROTECTION OFFICERS

There is not yet a requirement in Turkey to appoint a data protection officer.

COLLECTION & PROCESSING

Pursuant to the LPPD, it is mandatory to comply with certain principles while collecting and processing personal data. In light of such principles collected personal data must be all of the following:

- Processed fairly and lawfully
- Accurate and up-to-date
- Processed for specific, explicit and legitimate purposes
- Relevant, adequate and not excessive
- Kept for a term necessary for purposes or for a term prescribed in relevant laws for which the data have been processed

Further, in principle, personal data cannot be processed without being collected and processed with explicit consent of the data subject. However, the LPPD stipulates certain exceptions where consent is not required. These are:

- Processing is expressly permitted by law
- Processing is necessary for protection of the life or physical integrity of the data subject or a third party, where the data subject is not physically or legally capable of giving consent
- Processing personal data of the contractual parties is necessary for the conclusion or the performance of a contract
- Processing is mandatory for the data controller to perform his / her legal obligation(s)
- Personal data has been made public by the data subject
- Processing is necessary in order to assign, use or protect a right
- Processing is necessary for the legitimate interests of data processor and this does not damage the rights of the data

subject

Pursuant to Article 10 of the LPPD, data controllers or their authorized persons have an obligation to inform data subjects during the collection of the personal data. The Communiqué on Procedures and Principles for Compliance with the Obligation to Inform published in the Official Gazette dated March 10, 2018, numbered 30356 sets forth the principles and procedures on the obligation to inform. As part of the collection of data from the data subject the controller is obliged to provide the data subject with the following information:

- Identity of the controller and of its representative, if any
- Purposes of the processing for which the data is intended
- Recipients of the data and the reasons for transfer
- Process of collecting data and the legal grounds
- Rights of the data subject

Where the data has not been obtained from the data subject, the controller shall provide the data subject with the above stated information as well as details of the categories of data concerned. According to the relevant Communiqué, the obligation to inform should be fulfilled within a reasonable time after collecting the personal data, or during the first contact if the personal data is obtained for communication purposes with the relevant persons, or at the very latest the time of the initial transfer if the personal data is to be transferred.

Processing of sensitive personal data without explicit consent of the data subject is generally forbidden, although sensitive data other than health and sexual life data can be processed without explicit consent of data subject if a law / legislation permits such processing. Under the LPPD, data controllers need to take adequate measures required for the processing of sensitive personal data and comply with the decisions and guides of the Personal Data Protection Board designating such adequate measures. *See also* Personal Data Protection Board Decision dated January 31, 2018, numbered 2018/10 on Adequate Measures to be taken by Data Controllers in Processing the Special Categories of Personal Data.

Health data and sexual life data can only be processed by natural persons who are under an oath of secrecy or by authorities for the purposes of protecting public health, preventive medicine, medical diagnosis, the provision of care and treatment services or planning, and the management and financing of healthcare services.

Deletion, destruction or anonymization of personal data

The Regulation on Deletion, Destruction or Anonymization of Personal Data ("Regulation on Deletion of Personal Data") was published in the Official Gazette dated October 28, 2017, and entered into force on January 1, 2018. This Regulation is crucially important for data controllers in terms of time limitations regarding deletion, destruction or anonymization of personal data.

Pursuant to the Regulation on Deletion of Personal Data, data controllers are required to prepare a personal data processing inventory and a personal data storage and destruction policy (Policy). Data controllers are also required to take measures to safeguard the data that they are processing, identify persons working in personal data storage and destruction processes, categorize personal data, store and destroy these data, and determine periodic destruction processes.

If the prerequisites for processing personal data provided under LPPD are not met, then the personal data must be deleted, destroyed or anonymized by the data controller (of its own accord or upon the application of related person). All actions related to the execution of this process must be recorded and these records shall be kept for at least three years.

In addition, if a data controller ceases to continue to meet the above conditions for processing personal data, then they must carry out a process of periodic destruction. Periodic destruction is the deletion, destruction or anonymization of personal data at recurring intervals specified in the relevant data controller's Policy. This period cannot exceed six months.

TRANSFER

The LPPD distinguishes between the transfer of personal data to third parties in Turkey and the transfer of personal data to third countries.

Transfer of personal data to third parties

In principle, personal data can be transferred to third parties with the explicit consent of the data subject. The conditions and exemptions applied to collection and processing of personal data also apply to the transfer of personal data to third parties.

Transfer of personal data to parties in third countries

In addition to the conditions and exemptions applied to the transfer of personal data to third parties, one of the following conditions shall exist for transfer of data to parties in third countries:

- The country to which personal data will be sent shall have sufficient level of protection.
- The data controllers in Turkey and in the target country shall undertake protection in writing and obtain the Personal Data Protection Board's permission.

The Personal Data Protection Board shall declare the countries having adequate level of protection. So far, the Personal Data Protection Board has not announced any country. However, the Personal Data Protection Board has announced the minimum clauses to be found in the undertakings of data controllers by setting out examples of undertaking where there is not an adequate level of protection in the country where personal data is transferred.

SECURITY

In light of the provisions of the LPPD and consistent with the principles of good faith, those entrusted with personal data are expected to ensure protection of such data. Under the LPPD, the data controller is required to ensure that appropriate technical and organizational measures are taken to prevent all illegal processing and to ensure the data is not destroyed, lost, amended, disclosed or transferred without authority. Such measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected. Additionally, the data controller has to carry out the necessary inspections on its own institution or organization in order to ensure the implementation of the LPPD.

Data controllers and data processors shall not disclose any personal data in contradiction with the provisions of LPPD and shall not use any personal data for any purposes except for the purpose of processing. This obligation continues after leaving their institution.

In addition, the LPPD enables data subjects to apply to data controllers by various means in relation to their rights stated in Article 11. Data controllers have an obligation to take every necessary administrative and technical measure effectively to finalize these applications in accordance with the LPPD and in good faith. The Communiqué on Procedures and Principles for Application to Data Controller dated March 10, 2018, numbered 30356 outlines the procedures of application.

BREACH NOTIFICATION

There is no general breach notification obligation under the LPPD. However, in the event that personal data is unlawfully obtained by others, the data controller must notify the Personal Data Protection Board and the data subject as soon as possible. If necessary, the Personal Data Protection Board may declare such situation on its website or in any other way it deems appropriate. To date, many of the breach notifications to the Personal Data Protection Board have been made available to the public.

Additionally, under the Regulation on the Protection of Personal Data in the Electronic Communications Sector and the Preservation of Privacy, companies providing an electronic communication service and / or providing an electronic communication network and operating the sub-structure (Operators), are obliged to inform the Personal Data Protection Authority in a timely and effective manner if there is a risk that violates the security of the network and the personal data.

Administrative fines of up to three percent of the net sales of the previous calendar year may be applied to the Operator, if the personal data is destroyed, altered, stored or recorded, processed or disclosed involuntarily, in an unauthorized manner or illegally.

ENFORCEMENT

The LPPD and the Turkish Criminal Code No. 5237 impose custodial sentences for the unlawful processing of data. The Turkish Civil Law No. 4721 grants the right to claim compensation for the unjust use of data and a number of other laws impose administrative fines.

Furthermore, the LLPD provides for administrative fines up to ₺1 million for those who act contrary to the requirements or rules in the LPPD.

Administrative fines between ₺5,000 and ₺20,000 shall be imposed for providers that do register with ETBIS (discussed below).

As mentioned above, administrative fines between ₺20,000 and ₺1 million shall be imposed on data controllers that do not register as required by the Regulation on the Registry of Data Controllers.

ELECTRONIC MARKETING

The Law on Regulation of Electronic Trade was published in the Official Gazette on November 5, 2014 (Electronic Trade Law). The Electronic Trade Law came into force on May 1, 2015. Secondary legislation (The Regulation on Electronic Trade) was published in the Official Gazette on August 26, 2015, and came into force on the same date.

Pursuant to the Electronic Trade Law, commercial electronic communications (electronic marketing) can only be sent by if prior consent (opt-in) has been obtained from recipients. Such consent may be obtained in writing or through means of electronic communication, although if the consent is taken in physical from, must contain the recipient's signature. Commercial electronic communications can be sent to craftsman and merchants without obtaining prior consent. The commercial electronic communication must comply with the consent obtained from recipients, and must contain the identity of the service provider, contact information (such as email, SMS, telephone number, fax number (depending on the type of commercial electronic communication)), and, if sent on behalf of a third party, information about that third party.

Consumers have the right to refuse a commercial electronic communication, and the service provider is obliged to allow the free transmission of the refusal. Commercial electronic communications to the recipient must cease within three business days of the receipt of refusal. Non-compliance with the above obligations is subject to administrative fines between ₺1,000 to ₺15,000.

The Communiqué on Electronic Trade Information System and Obligations of Notification (Communiqué) was published in the Official Gazette on August 11, 2017, and entered in force on the same date. The Communiqué regulates the procedure and principles related to the registration and notifications through the Electronic Trade Information System (ETBIS), in respect of service providers operating in electronic trade (e-trade) and intermediary service providers that provide e-trade environments for the economic and commercial activities of others. Within the scope of the Communiqué, service providers and intermediary service providers are required to enroll in ETBIS before starting e-commerce activities. Service providers and intermediary service providers must provide information about the service, type of goods and services offered, payment methods and the like.

Similar regulations are enacted under electronic trade law. Accordingly, the obligation of registration and notification to ETBIS is imposed on service providers and intermediaries possessing certain qualifications. With regards to the Communiqué, service providers and intermediary service providers were obliged to fulfill this obligation between December 1, 2017, and December 31, 2017.

Administrative fines between ₺5,000 and ₺20,000 shall be imposed on providers that do not register with the ETBIS.

The Ministry of Customs and Trade is empowered to establish an electronic system that allows the receipt of commercial electronic communications approvals and the use of the right to refuse. The approvals received under the Electronic Trade Law shall be transferred to the system within the time limit set by the Ministry. The right of rejection by buyers is through this system. Other procedures and principles regarding the establishment of the system, the transfer of the approvals to the system, the use of the right to refuse, and the operation of the system will be determined by secondary legislation.

Since electronic marketing activities include more and more use of personal data, the Electronic Trade Law and the LPPD often may be implicated at the same time. The Personal Data Protection Board Decision dated October 16, 2018 numbered 2018/119 states that commercial electronic communications such as advertisement notifications and marketing telephone calls also fall within

the scope of the LPPD. However, this decision raised some questions regarding the application and enforcement of the Electronic Trade Law and LPPD at the same time, especially in relation to fines which may be imposed twice both according to the LPPD and the Electronic Trade Law.

ONLINE PRIVACY

There is no legislation in Turkey that specifically regulates privacy in respect of cookies and location data. However, Law No. 5651 on Regulating Broadcasting in the Internet and Fighting against Crimes Committed through Internet Broadcasting enables Internet users to initiate prosecution in case of infringements of their personal rights.

Under the Regulation on Protection of Personal Data in the Electronic Communications Sector and Preservation of Privacy, an Operator cannot process traffic data for purposes other than those required for the purposes of their service. Traffic data shall be processed in accordance with the provisions of the relevant legislation for the purposes of traffic management, interconnection, billing, corruption detection and similar transactions or settlement of disputes. The processed and stored traffic data belonging to the subscriber / user shall be deleted or made anonymous after the completion of the required activity to process and store these data.

Traffic data may be processed if required for marketing electronic communication services or providing value added electronic communication services, provided that either it is anonymized, or relevant subscribers / users give their consent after being informed of the traffic data to be processed and the processing time.

Location data not qualifying as traffic data may be processed if required to provide value added electronic communication services, on the condition that it is anonymized or the relevant subscribers / users give their consent after being informed of the location data to be processed and of the purpose and duration of the processing.

Administrative fines of up to three percent of the net sales of the Operator in the previous calendar year shall be imposed if it fails to fulfill its obligation to process traffic data and location data.

KEY CONTACTS

Burak Özdastanli
Partner
T +90 216 663 60 11
bozdagistanli@iptech-legal.com

Hatice Ekici Taa
Partner
T +90 216 663 60 11
hekici@iptech-legal.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

TURKMENISTAN

Last modified 28 January 2019

LAW

The Law of Turkmenistan No.519-V 'On Information about Private Life and its Protection' (the 'Data Protection Law') is the main and only law governing matters relating to collection and processing of personal data in Turkmenistan.

The Data Protection Law was enacted on 20 March 2017, ie after the adoption of the General Data Protection Regulation (the 'GDPR') and entered into force on 1 July 2017. In fact, the Data Protection Law partly reflects the rules and principles perpetuated in the GDPR. However, the similarities that can be discovered between the Data Protection Law and the GDPR are few and in most cases the Data Protection Law implements the simplified approach suggested by the GDPR.

DEFINITIONS

Article 1 of the Data Protection Law defines the term 'personal data' as 'any kind of information, which relates to a certain individual, which is recorded on an electronic, paper or other medium'. In terms of accessibility, personal data can be divided into two types: public (such as telephone directory, social media, etc) and restricted. Publicly available personal data includes information, which is either freely accessible upon consent of the individual (owner of personal data) or exempted from confidentiality in accordance with the laws of Turkmenistan.

The Data Protection Law additionally introduces a term 'biometric data' that encompasses any information that reflects physical and biological characteristics of an individual (owner of personal data). The term is somewhat similar to the term 'biometric data' that is envisaged in the GDPR (Article 4(14)) but does not include any reference to physiological and behavioural characteristics.

Both personal data and biometric data are recognized as confidential under the Data Protection Law and collection and processing of such data must be limited to the purposes the data is collected for.

In Turkmenistan the Data Protection Law does not provide for a definition of sensitive personal data. It is directly prohibited to collect specific categories of personal data which, inter alia, includes data on nationality, skin colour, religious and political views, medical conditions, etc. Collection of such categories of personal data is permissible under the following circumstances:

- Receipt of a written consent of owner of personal information
- Such personal data is publicly available
- Collection of personal data is required for healthcare and health protection of an owner of such personal data
- Collection of personal data is performed by religious or non-commercial organization provided that the collected data would not be distributed without a prior written consent of owner of personal data
- Collection of personal data is required for implementation of justice and / or investigative activity

NATIONAL DATA PROTECTION AUTHORITY

There is no special national authority in the field of data protection policy.

REGISTRATION

No registration of a personal data database is required under the Data Protection Law.

DATA PROTECTION OFFICERS

No appointment of a data protection officer is required under the Data Protection Law.

COLLECTION & PROCESSING

Owner of personal data shall give consent on collection and processing of its personal data. Such consent can be delivered in written or electronic form or by virtue of any other secured means in compliance with Turkmen law.

Any such consent shall include the following information:

- Name (surname, name), address, ID document of an owner of personal data
- Name (surname, name) and the address of the data operator
- Purpose of collecting and processing personal data
- List of personal data to be collected and processed by the data operator
- List of actions related to personal data for the purpose of which the consent is given, a general description of the methods used to collect and process personal data
- Term of the given consent, as well as the procedure for its withdrawal

No consent is required for collection and processing of personal data for the following purposes:

- Investigatory activity
- Statistical analysis
- Life and health protection, protection of constitutional rights
- Implementation of international agreements of Turkmenistan, etc

TRANSFER

For the purposes of cross-border transfers of personal data, the relevant consent of owner of personal data is required. Since the Data Protection Law does not stipulate on whether this should be a separate consent, it is recommended to obtain such consent together with a general consent on collection and processing of personal data.

Please note that personal data transferred outside Turkmenistan shall also be stored in the territory of Turkmenistan. Personal data processed for the purpose of statistical and/or scientific analysis shall be de-personalized.

Data operator is not allowed to transfer personal data outside Turkmenistan to a third party by virtue of a contract on collection and/or processing of personal data.

SECURITY

Article 23 of the Data Protection Law stipulates that data operators shall implement a set of legal, organizational and technical measures to ensure personal data protection. Such measures shall:

- Uphold the rights to privacy, personal and family secrets
- Ensure integrity and security of personal data
- Confidentiality of personal data
- Allow owner of personal data to have guaranteed access to such personal data
- Prevent unauthorised collection and processing of personal data

Data operators are statutorily obliged to take any necessary and lawful measures to protect personal data and ensure:

- Prevention of unauthorized access to personal data

- Timely detection of unauthorized access to personal information
- No adverse effects of such unauthorized access to personal data

It is important to note that the obligation of the data operators, as well as any third party acquiring the personal data, to protect confidentiality of the acquired personal data, arises from the moment such data is collected and shall be effective until the moment such data is destroyed or depersonalized.

BREACH NOTIFICATION

Data Protection Law does not provide for any provisions regarding breach notification requirements. In other words, data operators are not obliged to notify the owners of personal data regarding any identified or potential confidentiality breach. However, the Data Protection Law envisages that data operators are obliged to block any personal data within one working day, if there is risk that a breach occurred.

ENFORCEMENT

General enforcement of the Data Protection Law is performed by the General Prosecutor's Office. However, any suffered party may file a suit directly to a court.

ELECTRONIC MARKETING

Article 5(8) of the Law of Turkmenistan 'On Advertising' prohibits distribution of any information protected by the law (including personal data) for advertising purposes.

ONLINE PRIVACY

Data Protection Law provisions apply to online privacy as well. There are no other specific regulations that govern online privacy in Turkmenistan. Data operator shall refer to rules and regulations specified in the Data Protection Law.

KEY CONTACTS

Kamilla Khamraeva
Associate
Centil Law Firm
T +998 71 120 4778
kamilla.k@centil.law

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UAE - ABU DHABI GLOBAL MARKET FREE ZONE

Last modified 28 January 2019

LAW

Note: Please also see UAE – General, UAE – DIFC, UAE – DHCC.

The Abu Dhabi Global Market (ADGM) implemented the ADGM Data Protection Regulations 2015 (DPR 2015). These were subsequently amended by Data Protection (Amendment) Regulation 2018.

DEFINITIONS

Definition of data controller

Any person in the ADGM (excluding a natural person acting in his capacity as a staff member) who alone or jointly with others determines the purposes and means of the processing of personal data.

Definition of data processor

Any person (excluding a natural person acting in his capacity as a staff member) who processes personal data on behalf of a data controller.

Definition of data subject

A natural person to whom personal data relate.

Definition of identifiable natural person

A natural person who can be identified, directly or indirectly, in particular by reference to

- An identification number, or
- One or more factors specific to his
    - Biological
    - Physical
    - Biometric
    - Physiological
    - Mental
    - Economic
    - Cultural, or
    - Social identity

Definition of personal data

Any information relating to an identified natural person or an identifiable natural person.

Definition of processing

Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as:

- Collection
- Recording
- Organization
- Storage
- Adaptation or alteration
- Retrieval
- Consultation
- Use
- Disclosure by transmission, dissemination or otherwise making available
- Alignment or combination
- Blocking
- Erasure, or
- Destruction

Definition of registrar

The Registrar is the ADGM Registration Authority.

Definition of sensitive personal data

Personal data revealing or concerning (directly or indirectly):

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Criminal record
- Tradeunion membership, and
- Health or sex life

NATIONAL DATA PROTECTION AUTHORITY

The Office of Data Protection (which forms part of the Registrar) is the official body with day-to-day responsibility for enforcement and administration of the DPR 2015 in the ADGM.

The Office of Data Protection
Authorities Building
ADGM Square
Al Maryah Island
Abu Dhabi
UAE
Data.Protection@adgm.com
+971 2 333 8888

REGISTRATION

Data controllers must register with the Office of Data Protection in order to be entitled to act in that capacity. Furthermore, data

controllers must notify the Office of Data Protection of the appointment and removal of a processor within the timeframe specified in the DPR 2015.

Data controllers must also establish and maintain records of any personal data processing operations or set of such operations intended to secure a single purpose or several related purposes.

DATA PROTECTION OFFICERS

There is no requirement under the DPR 2015, for organizations to appoint a data protection officer, though note the general obligation of a data controller to implement appropriate technical and organizational measures to protect personal data, as further detailed below (see separate section on Security). It is however recommended that an organization that operates on a large scale or carries out regular and systematic monitoring of individuals appoint an individual responsible for overseeing the organization's compliance with data protection requirements.

COLLECTION & PROCESSING

Data controllers may process personal data when any of the following conditions are met:

- The data subject has given his written consent to the processing of that personal data (Article 2(a), DPR 2015).
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (Article 2(b), DPR 2015).
- Processing is necessary for compliance with any regulatory or legal obligation to which the data controller is subject (Article 2(c), DPR 2015).
- Processing is necessary in order to protect the vital interests of the data subject (Article 2(d), DPR 2015).
- Processing is necessary for the performance of a task carried out in the interests of the ADGM or in the exercise of the functions or powers of one of its official bodies (as specified in the DPR 2015) vested in the data controller or in a third party to whom the personal data are disclosed (Article 2(e), DPR 2015).
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party to whom the personal data are disclosed, except where such interests are overridden by compelling legitimate interests of the data subject relating to the data subject's particular situation (Article 2(f), DPR 2015).

Data controllers may process sensitive personal data when any of the following conditions are met:

- The data subject has given an additional written consent to the processing (Article 3(1)(a), DPR 2015).
- Processing is necessary for the purposes of carrying out the obligations and specific rights of the data controller (Article 3(1)(b), DPR 2015).
- Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent (Article 3(1)(c), DPR 2015).
- Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other nonprofit-seeking body on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed to a third party without the consent of the data subjects (Article 3(1)(d), DPR 2015).
- The processing relates to personal data which are manifestly made public by the data subject, or is necessary for the establishment, exercise or defense of legal claims (Article 3(1)(e), DPR 2015).
- Processing is necessary for compliance with any regulatory or legal obligation to which the data controller is subject (Article 3(1)(f), DPR 2015).
- Processing is necessary to uphold the legitimate interests of the data controller recognized in the international financial markets, provided the processing is undertaken in accordance with applicable standards and except where such interests are overridden by compelling legitimate interests of the data subject relating to the data subject's particular situation (Article 3(1)(g), DPR 2015).
- Processing is necessary to comply with any regulatory, auditing, accounting, anti-money laundering or counter-terrorist financing obligations that apply to a data controller or for the prevention or detection of any crime (Article 3(1)(h), DPR 2015).
- Processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or

the management of healthcare services, and where those personal data are processed by a health professional subject under law or rules established by competent bodies to the obligation of confidence or by another person subject to an equivalent obligation (Article 3(1)(i), DPR 2015).

Note, however, that sensitive personal data may be processed by a data controller irrespective as to whether any of the above have been satisfied if both of the following conditions are satisfied:

- A permit has been obtained from the Registrar to process sensitive personal data.
- The data controller applies adequate safeguards with respect to the processing of the personal data (Article 3(2), DPR 2015).

TRANSFER

Transfers of personal data outside of the ADGM may take place where there is an adequate level of protection for personal data, ensured by the laws and regulations applicable to the recipient. The jurisdictions deemed to have an adequate level of protection are set out in Schedule 3 to the ADGM Data Protection Regulations and this list may be added to by the Office of Data Protection over time (we are not aware of any additional countries having been added to the list).

In the absence of an adequate level of protection, data controllers may transfer personal data out of the ADGM if:

- The Registrar has granted a permit for the transfer or the set of transfers and the data controller applies adequate safeguards with respect to the protection of such personal data (Article 5(1)(a), DPR 2015)
- The data subject has given his written consent to the proposed transfer (Article 5(1)(b), DPR 2015)
- The transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of precontractual measures taken in response to the data subject's request (Article 5(1)(c), DPR 2015)
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party (Article 5(1)(d), DPR 2015)
- The transfer is necessary for the establishment, exercise or defense of legal claims (Article 5(1)(e), DPR 2015)
- The transfer is necessary in order to protect the vital interests of the data subject (Article 5(1)(f), DPR 2015)
- The transfer is necessary in the interests of the ADGM (Article 5(1)(g), DPR 2015)
- The transfer is made at the request of a regulator, the police or other government agency (Article 5(1)(h), DPR 2015)
- The transfer is made from a register which according to law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case (Article 5(1)(i), DPR 2015)
- The transfer is necessary for compliance with any regulatory or legal obligation to which the data controller is subject (Article 5(1)(j), DPR 2015)
- The transfer is necessary to uphold the legitimate interests of the data controller recognized in the international financial markets, provided that the transfer is carried out in accordance with applicable standards and except where such interests are overridden by legitimate interests of the data subject relating to the data subject's particular situation (Article 5(1)(k), DPR 2015)
- The transfer is necessary to comply with any regulatory, auditing, accounting, antimoney laundering or counter-terrorist financing obligations that apply to a data controller which is established in the ADGM, or for the prevention or detection of any crime (Article 5(1)(l), DPR 2015)
- The transfer is made to a person established outside the ADGM who would be a data controller (if established in the ADGM) or who is a data processor, if, prior to the transfer, a legally binding agreement in the form set out in Schedule 1 or Schedule 2 respectively of the DPR 2015 has been entered into between the transferor and recipient (Article 5(1)(m), DPR 2015)
- The transfer is made between members of a company group in accordance with a global data protection compliance policy of that group, under which all the members of such group that are or will be transferring or receiving the personal data are bound to comply with all the provisions of the ADGM Data Protection Regulations as if such group members were established in the ADGM *(ie,* effectively, Binding Corporate Rules) (Article 5(1)(n), DPR 2015)

SECURITY

Data controllers must implement appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing and against accidental loss or destruction of, or damage to, such personal data (Article 9(1), DPR 2015).

The measures implemented ought to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected (Article 9(2), DPR 2015).

Data controllers, when appointing a data processor, must ensure that the data processor provides sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and shall ensure compliance with those measures (Article 9(3), DPR 2015).

BREACH NOTIFICATION

In the event of a breach of any personal data held by a data processor, the data processor shall inform the data controller of the incident as soon as reasonably practicable (Article 9(4), DPR 2015).

If a data controller becomes aware of any breach of any personal data under its control, the data controller must inform the Registrar of the incident without undue delay, and where feasible, no later than 72 hours after becoming aware of it (Article 9(5), DPR 2015).

ENFORCEMENT

In the ADGM, the Office of Data Protection (forming part of the Registrar) oversees the enforcement of the DPR 2015.

The Office of Data Protection has the power under the DPR 2015 to:

- Issue directions or warnings and make recommendations to data controllers (Article 14(1)(d), DPR 2015)
- Impose fines in the event of non-compliance with its direction (Article 14(1)(e), DPR 2015)
- Impose fines in the event of non-compliance with the DPR 2015 and any rules made pursuant to them (Article 14(1)(f), DPR 2015)

If the Office of Data Protection is satisfied that a data controller has contravened or is contravening the DPR 2015, it may issue a direction to the data controller requiring it to do either or both of the following:

- To do or refrain from doing any act or thing within such time as may be specified in the direction (DPR 2015, Article 17(1)(a))
- To refrain from processing any personal data specified in the direction or to refrain from processing personal data for a purpose or in a manner specified in the direction (DPR 2015, Article 17(1)(b))

A data controller who receives a fine from the Office of Data Protection for its contravention of the DPR 2015 may refer such matter to the ADGM courts for review to contest either the issue of the fine or the amount of the fine (Article 17A(7), DPR 2015).

ELECTRONIC MARKETING

Immediately upon commencing to collect personal data, the DPR 2015 requires data controllers to provide data subjects who they have collected personal data from, with, among other things, any further information to the extent necessary (with respect to the specific circumstances in which the personal data is collected). This includes information on whether the personal data will be used for direct marketing purposes (Article 6(1)(c)(iv), DPR 2015).

If the personal data has not been obtained from the data subject, the data controller (or their representative) must at the time of processing the personal data provide the data subject with, among other things, information regarding whether the personal data will be used for direct marketing purposes.

If it is envisaged that the personal data will be disclosed to a third party, this must be done no later than when the personal data is first disclosed to that third party (Article 7(1)(c)(iv), DPR 2015).

Before personal data is disclosed for the first time to third parties or used on a data subject's behalf for the purposes of direct marketing, data subjects also have the right to be informed and to be expressly offered the right to object to such disclosures or uses (Article 11(1)(b), DPR 2015).

ONLINE PRIVACY

The DPR 2015 does not contain specific provisions relating to online privacy, however, the broad provisions detailed above are likely to apply. In addition, as UAE criminal law applies in the ADGM, the privacy principles laid out therein may apply (see UAE – General).

KEY CONTACTS

Paul Allen
Head of Intellectual Property & Technology – Middle East
T +971 4 438 6295
paul.allen@dlapiper.com

Eamon Holley
Legal Director
T +971 4 438 6293
eamon.holley@dlapiper.com

Jamie Ryder
Senior Legal Consultant
T +971 4 438 6297
jamie.ryder@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UAE - DUBAI (DIFC)

Last modified 28 January 2019

LAW

Note: Please also see UAE – General, UAE – ADGM, UAE – DHCC.

The Dubai International Financial Centre (DIFC) implemented DIFC Law No. 1 of 2007 Data Protection Law in 2007 which was subsequently amended by DIFC Law No. 5 of 2012 Data Protection Law Amendment Law (DPL).

In addition, under the powers granted to the Commissioner of Data Protection (CDP) under Article 28 of the DPL, the CDP has issued the Data Protection Regulations (DPR).

DEFINITIONS

Definition of personal data

Any data referring to an identifiable natural person

Definition of identifiable natural person

A natural living person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity

Definition of sensitive personal data

Personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life

Definition of process, processed, processes and processing

Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

NATIONAL DATA PROTECTION AUTHORITY

The Commissioner of Data Protection (CDP) is essentially the regulating body in the DIFC.

The Data Protection Commissioner
Dubai International Financial Centre Authority

Level 14, The Gate
P.O. Box 74777
Dubai
United Arab Emirates

administrator@dp.difc.ae

Tel: +971 4 362 2623
Fax: +971 4 362 2656

REGISTRATION

Unless certain exceptions apply, data controllers must obtain a permit from the CDP prior to commencing a processing operation involving either sensitive personal data or transferring personal data outside of the DIFC.

Data controllers must also notify the CDP of any processing operations involving either sensitive personal data or the transfer of personal data outside of the DIFC.

DATA PROTECTION OFFICERS

There is no requirement under the DPL or the DPR, for organizations to appoint a data protection officer, though note the general obligation of a data controller to implement appropriate technical and organizational measures to protect personal data, as further detailed below (see separate Security section).

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

- The data subject has given his / her written consent to the processing of that personal data (DPL, Article 9(a))
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (DPL, Article 9(b))
- Processing is necessary for compliance with any legal obligation to which the data controller is subject (DPL, Article 9(c))
- Processing is necessary for the performance of a task carried out in the interests of the DIFC, or in the exercise of the DIFC Authority, the Dubai Financial Services Authority, the Court and the Registrar's functions or powers vested in the data controller or in a third party to whom the personal data are disclosed (DPL, Article 9(d))
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the personal data is disclosed, except where such interests are overridden by compelling legitimate interests of the data subject relating to the data subject's particular situation (DPL, Article 9(1)(e))

Data controllers may collect and process sensitive personal data when any of the following conditions are met:

- The data subject has given his / her written consent to the processing of that sensitive personal data (DPL, Article 10(1)(a))
- Processing is necessary for the purposes of carrying out the obligations and specific rights of the data controller (DPL, Article 10(1)(b))
- Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent (DPL, Article 10(1)(c))
- Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other nonprofit-seeking body on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed to a third party without the consent of the data subjects (DPL, Article 10(1)(d))
- The processing relates to personal data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims (DPL, Article 10(1)(e))
- Processing is necessary for compliance with any regulatory or legal obligation to which the data controller is subject (DPL, Article 10(1)(f))

- Processing is necessary to uphold the legitimate interests of the data controller recognized in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by compelling legitimate interests of the data subject relating to the data subject's particular situation (DPL, Article 10(1)(g))
- Processing is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter-terrorist financing obligations or the prevention or detection of any crime that apply to a data controller (DPL, Article 10(1)(h))
- Processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those personal data is processed by a health professional subject under national laws or regulations established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy (DPL, Article 10(1)(i))
- Processing is required for protecting members of the public against dishonesty, malpractice or other seriously improper, or any resultant financial loss (DPL, Article 10(1)(j))
- Authorized in writing by the CDP (DPL, Article 10(1)(k))

TRANSFER

Data controllers may transfer personal data out of the DIFC if the personal data is being transferred to a Recipient in a jurisdiction that has laws that ensure an adequate level of protection for that personal data (DPL, Article 11(1)(a)). An adequate level of protection is when the level of protection in that jurisdiction is acceptable pursuant to the DPR or any other jurisdiction approved by the CDP (DPL, Article 11(2)).

In the absence of an adequate level of protection, data controllers may transfer personal data out of the DIFC if the:

- CDP has granted a permit or written authorization for the transfer or the set of transfers and the data controller applies adequate safeguards with respect to the protection of this personal data (DPL Article 12(1)(a)). Article 5.1 of the DPR then sets out the requirements for applying for such a permit (including a description of the proposed transfer of personal data for which the permit is being sought and including a description of the nature of the personal data involved)
- Data subject has given his / her written consent to the proposed transfer (DPL, Article 12(1)(b))
- Transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken in response to the data subject's request (DPL, Article 12(1)(c))
- Transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party (DPL, Article 12(1)(d))
- Transfer is necessary or legally required on grounds important in the interests of the DIFC, or for the establishment, exercise or defense of legal claims (DPL, Article 12(1)(e))
- Transfer is necessary in order to protect the vital interests of the data subject (DPL, Article 12(1)(f))
- Transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case (DPL, Article 12(1)(g))
- Transfer is necessary for compliance with any legal obligation to which the data controller is subject or the transfer is made at the request of a regulator, police or other government agency (DPL, Article 12(1)(h))
- Transfer is necessary to uphold the legitimate interests of the data controller recognized in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by legitimate interests of the data subject relating to the data subject's particular situation (DPL, Article 12(1)(i))
- Transfer is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter-terrorist financing obligations or the prevention or detection of any crime that applies to a data controller (DPL, Article 12(1)(j))

Authorities who may receive personal data in the context of a particular inquiry are not regarded as Recipients under the DPL or the DPRs (as per the definition of Recipient in the DPL).

Transfer to the United States

The DIFC notes on its list of adequate data protection regimes that as the EU-US Privacy Shield, which replaced Safe Harbor in 2016, is a mechanism recognized by the European Commission for transferring personal data between the EU/EEA and the USA only, the DIFC does not recognize it for this reason, as DIFC has no such agreement in place with the USA for transfers of personal data from the DIFC to the USA. Therefore the US Privacy Shield is not an option for transfers from the DIFC to the USA (or elsewhere).

If personal data originating in the DIFC is transferred to the EU and then transferred onward to the USA, then the Privacy Shield come into play if the transferring organization has the appropriate Privacy Shield certification. Privacy Shield is currently under review by the DIFC for effectiveness.

SECURITY

Data controllers must implement appropriate technical and organizational measures to protect personal data against willful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing, in particular where sensitive personal data is being processed or where the personal data is being transferred out of the DIFC (to a jurisdiction without an adequate level of protection) (DPL, Article 16(1)). When applying for a permit to process sensitive personal data, or transfer personal data out of the DIFC, data controllers must include detail regarding the safeguards employed to ensure the security of such sensitive personal data (respectively, Articles 2.1.1(i) and 5.1.1(i) of the DPR).

The measures implemented ought to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected (DPL, Article 16(2)).

BREACH NOTIFICATION

In the event of a breach (being an unauthorized intrusion, either physical, electronic or otherwise, to any personal data database, as defined by the DPL) data controllers (or data processors carrying out a data controller's function at the time of the breach), must inform the CDP of the incident as soon as reasonably practicable (DPL, Article 16(4)).

ENFORCEMENT

In the DIFC, the CDP oversees the enforcement of the DPL (DPL, Article 26).

The CDP needs to conduct all reasonable and necessary inspections and investigations before notifying a data controller that it has breached or is breaching the DPL or any regulations (DPL, Article 33). If the CDP is satisfied with the evidence of the breach, the CDP may issue a direction to the data controller requiring it to do either or both of the following:

- Do or refrain from doing any act or thing within such time as may be specified in the direction (DPL, Article 33(1)(a))
- Refrain from processing any personal data specified in the direction or to refrain from processing personal data for a purpose or in a manner specified in the direction (DPL, Article 33(1)(b))

A data controller may ask the CDP to review the direction within 14 days of receiving a direction and the CDP may receive further submissions and amend or discontinue the direction (DPL, Article 33(6)).

A data controller that fails to comply with a direction of the CDP may be subject to fines and liable for payment of compensation (DPL, Article 33(4)).

In addition, if the CDP considers that a data controller or any officer of it has failed to comply with a direction, he may apply to the Court for one or more of the following orders:

- An order directing the data controller or officer to comply with the direction or any provision of the Law or the Regulations or of any legislation administered by the CDP relevant to the issue of the direction (DPL, Article 33(5)(a))
- An order directing the data controller or officer to pay any costs incurred by the CDP or other person relating to the issue of the direction by the CDP or the contravention of such Law, Regulations or legislation relevant to the issue of the direction (DPL, Article 33(5)(b))

- Any other order that the Court considers appropriate. (DPL, Article 33(5)(c))

Any data controller who is found to contravene the DPL or a direction of the CDP may appeal to the DIFC Court within 30 days (DPL, Article 37(1)). The DIFC Court may make any orders that it thinks just and appropriate in the circumstances, including remedies for damages, penalties or compensation (DPL, Article 37(2)).

ELECTRONIC MARKETING

As soon as possible upon beginning to collect personal data, the DPL requires data controllers to provide data subjects who they have collected personal data from, with, among other things, any further information to the extent necessary (with respect to the specific circumstances in which the personal data is collected). This includes information on whether the personal data will be used for direct marketing purposes (DPL, Article 13).

If the personal data has not been obtained from the data subject, the data controller or their representative must at the time of processing provide the data subject with, among other things, information regarding whether the personal data will be used for direct marketing purposes. If it is envisaged that the personal data will be disclosed to a third party, this must be done no later than when the personal data is first processed or disclosed (DPL, Article 14).

Before personal data is disclosed for the first time to third parties or used on a data subject's behalf for the purposes of direct marketing, data subjects also have the right to be informed and to be expressly offered the right to object to such disclosures or uses (DPL, Article 18).

Additionally, the DPL requires a data controller to record various types of information regarding its personal data processing operations (Article 19(4)). This must include an explanation of the purpose for the personal data processing (DPL, Article 6.1.1(b)). The DPR suggests that one of these purposes may be for advertising, marketing and public relations for the data controller itself or for others (Article 6.2.1).

ONLINE PRIVACY

The DPL or DPR do not contain specific provisions relating to online privacy, however, the broad provisions detailed above are likely to apply. In addition, as UAE criminal law applies in the DIFC, the privacy principles laid out therein may apply. (see UAE - General section).

KEY CONTACTS

Paul Allen
Head of Intellectual Property & Technology – Middle East
T +971 4 438 6295
paul.allen@dlapiper.com

Eamon Holley
Legal Director
T +971 4 438 6293
eamon.holley@dlapiper.com

Jamie Ryder
Senior Legal Consultant
T +971 4 438 6297
jamie.ryder@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UAE - DUBAI HEALTH CARE CITY FREE ZONE

Last modified 28 January 2019

LAW

Note: Please also see UAE – General, UAE – DIFC, UAE – ADGM.

The Dubai Healthcare City (DHCC), a healthcare free zone in Dubai, implemented DHCC Health Data Protection Regulation No 7 of 2013 (which repealed and replaced the DHCC Data Protection regulation No. 7 of 2008) (HDPR).

The HDPR regulates the protection of Patient Health Information, as opposed personal data. The HDPR applies to healthcare professionals working in the DHCC with access to Patient Health Information (Licensees), including any of the following:

- Licensed Healthcare Professional
- Licensed Complementary and Alternative Medicine Professional
- Licensed Healthcare Operator
- Approved Education Operator
- Approved Research Operator
- Licensed Commercial Company
- Non-Clinical Operating Permit Holder

DEFINITIONS

Definition of personal data

The relevant defined term is '**Patient Health Information**' which is defined as information about a patient — whether spoken, written, or contained in an electronic record — that is created or received by any Licensee, that relates to the physical or mental health or condition of the patient, including the reports from any diagnostic procedures and information related to the payment for services.

Definition of process, processed, processes and processing

Any operation or set of operations that is performed on Patient Health Information, whether or not by automatic means, such as:

- Collection
- Recording
- Organization
- Storage
- Adaptation or alteration
- Retrieval

- Consultation
- Use
- Disclosure by transmission
- Dissemination or otherwise making available
- Alignment
- Erasure
- Destruction

NATIONAL DATA PROTECTION AUTHORITY

The DHCC Board of Directors and the Executive Body of the Dubai Healthcare City Authority (DHCA) are responsible for ensuring proper administration of the HDPR and any rules, standards and policies made under the HDPR.

The Centre for Healthcare Planning and Quality is responsible for the compliance and enforcement of the HDPR (CPQ).

Dubai Healthcare City Authority - Regulatory
Tel: +971-4-3838300
Fax: +971-4-3838300
info@dhcr.gov.ae

REGISTRATION

Not applicable.

DATA PROTECTION OFFICERS

There is a requirement for each Licensee to have at least one Data Protection Officer.

Data Protection Officer responsibilities include:

- Encouraging the Licensee's compliance with the HDPR
- Dealing with requests made to the Licensee under the HDPR
- Otherwise ensuring compliance by the Licensee with the provisions of the HDPR (section 40 HDPR)

COLLECTION & PROCESSING

Patient Health Information is not permitted to be collected by any Licensee unless it is for a lawful purpose and the collection is necessary for that purpose (article 27 HDPR). However, the meaning of lawful purpose is not defined in the HDPR.

Patient Health Information should be collected from the patient directly unless the Licensee has reasonable grounds to believe any of the following things to be true:

- That the patient concerned authorizes collection of the information from someone else having been made aware of the matters set out in section 29(1)
- That the patient is unable to give his or her authority, and the Licensee—having made the patient's representative aware of the matters set out in section 29(1)—collects the Patient Health Information from the representative (or the representative authorizes collection from someone else)
- That compliance would prejudice the:
    - Interests of the patient
    - Purposes of collection, or
    - Safety of any individual
- That compliance is not reasonably practicable in the circumstances of the particular case
- That the collection is for the purpose of assembling a family or genetic history of a patient and is collected directly from that patient and / or the patient's representative

- That the Patient Health Information is publicly available information
- That the Patient Health Information:
    - Will not be used in a form in which the patient is identified
    - Will be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the patient, or
    - Will be used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the patient
- That non-compliance is necessary:
    - To avoid prejudice to the maintenance of the law including the prevention, detection, investigation, prosecution and punishment of offenses
    - For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation) (section 28 HDPR)

TRANSFER

Patient Health Information may only be transferred to a third party located in a jurisdiction outside DHCC if all of the following conditions are satisfied:

- An adequate level of protection for that Patient Health Information is ensured by the laws and regulations that are applicable to the third party
- The transfer is either:
    - Authorized by the patient
    - Necessary for the ongoing provision of Healthcare Services to the patient

A jurisdiction shall be considered to have an adequate level of protection if that jurisdiction is listed as an acceptable jurisdiction under the Dubai International Financial Center Data Protection Law No. 1 of 2007, or has the written approval of the Central Governance Board.

The DHCC Healthcare Data Protection Regulation of 2008 contained a provision which permitted the transfer of Patient Heath Information to a jurisdiction without adequate protection, if a permit was sought.

However, this was removed under the HDPL and the Central Government Board does not have the power to issue permits for the transfer to jurisdictions without an adequate level of protection.

SECURITY

A Licensee is responsible for the security of its information systems and networks and should act in a timely and cooperative manner to prevent, detect and respond to security incidents. A Licensee is further required review and assess the security of information systems and networks and make appropriate modifications to security policies, practices, measures and procedures on a regular basis. Any security incidents must be disclosed to the CPU on a periodic basis.

A Licensee that holds Patient Health Information must maintain the security of the Patient Health Information, ensuring that it is stored in a way that can be readily retrieved and easily removed or shared, while also protecting the accuracy of the information.

A Licensee is further responsible for ensuring that reasonable safeguards are put in place to protect the Patient Health Information from:

- Loss
- Destruction
- Potential fire / water damage
- Tampering
- Theft
- Unauthorized access, use, modification or disclosure

(section 31, HDPR)

BREACH NOTIFICATION

There is no specific requirement set out in the DPL obliging a Licensee to inform the CPQ in the event of a breach. Licensees are required to inform the Customer Protection Unit (within CPQ) on a periodic basis of any security incidents.

ENFORCEMENT

The CPQ is responsible for the compliance and enforcement of the HDPR and may delegate its powers and duties to any appropriate committee(s) constituted by it, or to appropriate person(s) appointed by it (section 42 HDPR).

The powers, duties and functions of CPQ include:

- Conducting an audit of Patient Health Information when requested by a Licensee for the purpose of ascertaining whether or not the information is maintained in accordance with the HDPR
- Monitoring the use of Personal Identifiers, and reporting to the Executive Body from time to time on the results of that monitoring, including any recommendations relating to the need for, or desirability of taking regulatory, administrative, or other action to give protection, or better protection, to the patient or the Licensee
- Monitoring compliance with the HDPR

CPQ may require a Licensee to produce specified information or documents when requested in writing in relation to the Processing of Patient Health Information of a complaint about an interference with Patient Health Information. If the Licensee does not comply with the request, the CPQ may impose a penalty as set out in a list to be published by the DHCA from time to time (section 42).

It does not appear that the DHCA have produced any further information on the penalties that apply in relation to a breach of HDPR. It is unclear how any breaches of the HDPR will be dealt with in the DHCC.

ELECTRONIC MARKETING

The HDPR does not contain specific provisions relating to electronic or direct marketing.

ONLINE PRIVACY

The HDPR does not contain specific provisions relating to online privacy, however, the broad provisions detailed above are likely to apply. In addition, as UAE criminal law applies in the DHCC, the privacy principles laid out therein may apply (see UAE – General).

KEY CONTACTS

Paul Allen
Head of Intellectual Property & Technology – Middle East
T +971 4 438 6295
paul.allen@dlapiper.com

Eamon Holley
Legal Director
T +971 4 438 6293
eamon.holley@dlapiper.com

Jamie Ryder
Senior Legal Consultant
T +971 4 438 6297
jamie.ryder@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UAE - GENERAL

Last modified 28 January 2019

LAW

Note: Please also see UAE – Dubai (DIFC), UAE – ADGM, UAE – DHCC.

The UAE does not have a comprehensive data protection law at its federal level, however there are a number of laws in place that govern privacy and data security in the UAE. There are also sector-specific data protection provisions in certain laws. The UAE also has a number of special economic or sector free zones, three of which have specific data protection laws. These are the Dubai International Financial Centre, the Abu Dhabi Global Market and the Dubai Health Care City.

The most relevant privacy law of general application in the UAE is Article 379 of the UAE Penal Code. This law prohibits a person who, by reason of their profession, craft, situation or art, is entrusted with a "secret," from using or disclosing that "secret," without the consent of the person to whom the secret pertains, or otherwise in accordance with the law.

A breach of this provision is punishable by criminal penalty of imprisonment of a minimum of one year, or a fine of a minimum of Twenty Thousand Dirhams, or both.

The term "secret" is undefined, however it is generally broadly construed to cover the concepts of personal data, as defined in many data protection laws (for example, name, date of birth, sex, religion etc.).

The terms "use" or "disclose" are also undefined, however the terms are again generally broadly construed to cover the concepts of "processing" and "transfer" respectively. Transfer can be to a third party or to another entity within the UAE or overseas.

Article 379 of the UAE Penal Code allows for the use or disclosure with the consent of the person to whom the secret pertains. Therefore, to mitigate against the risk of a breach of Article 379 of the Penal Code it is generally advised to obtain such consent prior to the use or disclosure of personal data. This can be done in a number of ways, depending upon the specific context of how the data is collected and used, for example by signature against a paper consent form, or by electronic signature or tick box against an electronic consent form.

On January 1, 2017, the UAE's Central Bank published the Regulatory Framework for Stored Values and Electronic Payment Systems (**Digital Payment Regulation**). This regulation governs digital payment service providers (**PSPs**) in the UAE, providing services such as cash-in services, cash out services, retail credit and debit digital payment transactions, government credit and debit digital payment transactions, peer-to-peer digital payment transactions and money remittances. PSPs are required to store all user identification data and transaction records. This data can only be made available to the corresponding User, the Central Bank, to other regulatory authorities following prior approval of the Central Bank, or by UAE court order. PSPs must not process or share the personal data provided by users, unless necessary as per anti-money laundering (**AML**) and combatting of financing terrorism (**CFT**) laws. PSPs must store and retain all user and transaction data exclusively within the borders of the UAE, excluding UAE financial Free Zones (the DIFC and ADGM), for a period of five years from the date the original transaction. No

user or transaction data can be stored outside of the UAE. Details of users' personal information must be stored for a minimum of five years from the date the user relationship is terminated.

In December 2015 the Dubai Government published the Dubai Law No. 26 of 2015 on the Regulation of Data Dissemination and Exchange in the Emirate of Dubai, ("Dubai Data Law"). The purpose of the Dubai Data Law to collate and manage data that relates to the emirate of Dubai and, where appropriate, to publish it as Open Data or at least ensure that it is shared it between authorized persons. This law is considered unique as it is likely the only one in the world that provides a government with power to require designated private sector entities to provide it with information held by the company in relation to a city, for purposes of making that information Open Data.

In addition, there are several UAE Federal Laws that contain various provisions in relation to privacy and the protection of personal data:

- Constitution of the UAE (Federal Law 1 of 1971)
- Penal Code (Federal Law 3 of 1987 as amended)
- Cyber Crime Law (Federal Law 5 of 2012 regarding Information Technology Crime Control) (as amended by Federal Law No. 12 of 2016 and Federal Decree Law No. 2 of 2018)
- Regulating Telecommunications (Federal Law by Decree 3 of 2003 as amended), which includes several implementing regulations/policies enacted by the Telecoms Regulatory Authority ('TRA') in respect of data protection of telecoms consumers in the UAE

DEFINITIONS

The concept of 'Personal Data', as understood in the EU, is not reflected under UAE Federal Law. The corresponding concept within UAE Law encompasses notions such as 'secrets', 'photographs', 'the privacy of the individual or family life' and 'private life or family life secrets of individuals'. As such, while no UAE Federal Law explicitly states that the collection of personal data requires express consent, if any such data pertains to private or family life then, in certain circumstances, the consent of the individual(s) concerned may be required.

The Digital Payment Regulation does not define User identification data, however other Central Bank regulations, such as AML and CFT rules, require, for example, that when banks open an account they obtain documentation to include the full name of the account holder, the current address and place of work as well as copies of the account holders passport.

NATIONAL DATA PROTECTION AUTHORITY

There is no National Data Protection Authority in the UAE. In respect of telecommunications services, the TRA is responsible for overseeing the relevant telecoms laws and policies.

The UAE Central Bank is responsible for the Digital Payment Regulation.

REGISTRATION

There are no data protection registration requirements in the UAE.

DATA PROTECTION OFFICERS

There is no requirement in the UAE for organizations to appoint a data protection officer.

COLLECTION & PROCESSING

If the collection and processing of any personal data pertains to an individual's private or family life then the consent of the individual may be required in certain circumstances. A failure to obtain such consent would constitute a breach of the Penal Code (Article 378 and 379) and could also be a breach of:

- Cyber Crime Law if the personal data is obtained or processed through the internet or electronic devices in general (Articles 21 and 22)

- Telecoms Law to the extent that data is obtained through any means of telecommunication, including through a telecommunications service provider, or any other electronic means. In addition, the facility should be made available for such consent to be withdrawn at a later stage (TRA Consumer Protection Regulations, Article 13.5)

The Cyber Crime Law criminalizes obtaining, possessing, modifying, destroying or disclosing (without authorization) electronic documents or electronic information relating to medical records (Article 7). Additionally, unlawful access via the Internet or electronic devices of financial information (*eg*, Credit Cards and Bank Accounts) without permission is an offense under Articles 12 and 13.

TRANSFER

Pursuant to the Penal Code (Article 379), personal data may be transferred to third parties inside and/or outside of the UAE if the data subjects have consented in writing to such transfer, or otherwise where allowed by law.

In addition, in circumstances where telecommunications service providers provide subscriber information to affiliates or third parties directly involved in the supply of the services requested by a subscriber, the third parties are required to take all reasonable and appropriate measures to protect the confidentiality and security of the information, and use such information only as needed for the provision of the requested services. Telecommunications service providers are required to ensure that the contracts between them and any affiliate or third party holds the other party responsible for the privacy and protection of the subscriber's information (TRA Consumer Protection Regulations, Article 13.8).

However, the requirement to obtain written consent may be waived, pursuant to the Penal Code (Article 377), where the personal data pertains to a crime to which the data subject is answerable and it is disclosed in good faith to the relevant authorities.

SECURITY

There are no specific provisions under UAE Federal Law relating to the type of measures to be taken or level of security to have in place against the unauthorized disclosure of personal data. Instead, the Cyber Crime Law focuses on offenses related to accessing data without permission and / or illegally (Articles 2 and 3), including financial information (*eg*, credit card information or bank account information) (Articles 12 and 13).

Article 13.1 of the TRA Consumer Protection Regulations requires telecommunications service providers to 'take all reasonable and appropriate measures to prevent the unauthorized disclosure or the unauthorized use of subscriber information'. Article 13.3 further stipulates that telecommunications service providers must take 'all reasonable measures to protect the privacy of Subscriber Information that it maintains in its files, whether electronic or paper form', and that 'reliable security measures' should be employed.

Based on the above, best practice from a UAE law perspective would be to take appropriate technical security measures against unauthorized or unlawful processing of, and against accidental disclosure of, personal data. The measures taken must ensure a level of security adequate enough to minimize the risk of liability arising out of a claim for breach of privacy made by a data subject.

BREACH NOTIFICATION

There is no mandatory requirement under UAE Federal Law to report data security breaches.

Data subjects based in the UAE, however, may be entitled to hold the entities in possession of their data liable under the principles of the UAE Civil Code for their negligence in taking proper security measures to prevent the breach, if such breach has resulted in actual losses being suffered by the data subjects.

In relation to telecommunication services, the Telecoms Law and most Policies do not include an explicit requirement on service providers to take the initiative in notifying the TRA of a breach or alleged breach, unless a subscriber complains to a service provider about the unauthorized disclosure of his or her personal data. Such a notification would be included in the monthly reporting which is submitted to the TRA (Article 15.10.2 of the TRA Consumer Protection Regulations).

Subscribers are also able to complain directly to the TRA about the unauthorized disclosure of their personal data. However, the TRA will generally only handle subscriber complaints after the complaint has been submitted to the service provider and if the matter has not been satisfactorily resolved by the service provider's own customer complaints procedure (Article 15.11.1 of the TRA Consumer Protection Regulations.

ENFORCEMENT

There are four possible methods of enforcement from a UAE law perspective:

1. Where the unauthorized disclosure of personal data results in a breach of the Penal Code:

The Public Prosecutor in either the Emirate:

- where the party suspected of the breach ('Offender') resides
- where the disclosure occurred

will have jurisdiction over a data subject's complaint.

If after concluding investigations with the police, the Public Prosecutor is satisfied with the evidence compiled, charges may be brought against the suspect.

The case would then be transferred to the Criminal Courts of First Instance. The data subject may attach a civil claim to the criminal proceedings before the Courts have ruled on the case.

Pursuant to the Penal Code (Article 379), if the Courts find a suspect guilty of disclosing secrets that were entrusted to him 'by reason of his profession, craft, situation or art' the penalties to be imposed under the Penal Code may include a fine of at least UAE Dirhams 20,000 (the fine is determined by the Courts) and / or an imprisonment for at least one year. More generally, pursuant to the Penal Code (Article 378), 'a punishment of confinement and fine shall be inflicted on any person who attacks the sanctity of individuals' private or family life' by committing any of the acts described under Article 378 'other than the legally permitted cases or without the victim's consent'.

When ruling on the criminal case, the Criminal Courts would usually transfer a civil claim made by the data subject to the Civil Courts of First Instance for further consideration. The data subject would need to prove the losses her or she has suffered as a direct result of the disclosure of his/her personal data before the Civil Courts in order for damages to be awarded.

2. Where the unauthorized disclosure of personal data results in a breach of the Cyber Crime Law:

The police in each Emirate have developed specialized cybercrime units to handle complaints that relate to breaches of the Cyber Crime Law.

As above, the cybercrime unit in the Emirate where:

- the Offender resides, or
- where the disclosure occurred

will have jurisdiction over a data subject's complaint.

The cybercrime unit would investigate the case and decide whether or not to refer it to the Public Prosecutor in the same Emirate. If the case is referred and the Public Prosecutor is satisfied with the findings of the cybercrime unit, charges would be brought against the suspect. The same procedure identified above is then followed before the Courts.

If found guilty of an offense under the Cyber Crime Law, the punishment an Offender can receive varies depending on the nature of the crime. Punishments range from temporary detention, a minimum prison sentence of between six months or one year and /

or a fine between AED 150,000 and AED 1,000,000 (Articles 2, 3, 7, 21 and 22 of the Cyber Crime Law). If found guilty of an attempt to commit any of the relevant offenses under the Cyber Crime Law, the punishment is half the penalty prescribed for the full crime (Article 40).

3. Where the unauthorized disclosure of personal data results in a breach of the Telecoms Law and Policies:

The TRA is responsible for overseeing the enforcement of the Telecoms Law and in this regard may rely on the Police and Public Prosecutor in the Emirate where, either:

- the breach has occurred, or
- where the suspect resides.

Where a licensed telecommunications service provider has breached the law, the subscriber / data subject generally needs to complain first to the service provider about the breach, though a direct approach to the TRA may be accepted by the them at their discretion (Article 15.11.1 of the TRA Consumer Protection Regulations).

The subscriber's complaint needs to be submitted to the TRA within three months of the date when the service provider last took action. This three months requirement may be waived subject to the discretion of the TRA (Article 15.11.1 of the TRA Consumer Protection Regulations).

After examining the complaint the TRA may direct the service provider 'to undertake any remedy deemed reasonable and appropriate' (Article 15.11.5 of the TRA Consumer Protection Regulations).

4. Where the unauthorized disclosure or transfer of personal data results in a breach of the Digital Payment Regulation:

The Central Bank will issue administrative penalties against PSPs. Currently the Digital Payment Regulation does not specify the administrative penalties.

ELECTRONIC MARKETING

There are no general laws in the UAE law covering electronic marketing, however the TRA has issued a regulation governing telecommunications licensees' electronic communications with subscribers, as well as how they should monitor spam passing through their networks. Articles 21 and 22 of the Cyber Crime Law and Article 13.5 of the TRA's Consumer Protection Regulation, as described in the 'Collection and Processing' section above, are also worded widely enough to potentially apply to electronic marketing. Article 22 of the Cyber Crime Law, for example, prohibits the use of various electronic devices in order to disclose, without permission, confidential information that has been obtained through the course of a person's duties.

The TRA's Unsolicited Electronic Communications Regulation states that telecommunications licensees are under a general obligation to put all practical measures in place to minimize the transmission of Spam having a UAE Link across their Telecommunications Networks, and where they are aware of Spam having a UAE Link sent to or from a particular Electronic Address, they must take all practical means to end the transmission of that Spam and to prevent the future transmission of such Spam. Spam is defined as Marketing Electronic Communications sent to a Recipient without obtaining the Recipient's Consent. Although the Unsolicited Electronic Communications Regulation is targeted and enforced against telecommunications licensees, it effectively puts an obligation upon the licensees to minimize and prevent Spam from being transmitted through their networks.

ONLINE PRIVACY

Although the UAE Penal Code does not contain provisions directly relating to the internet, its provisions related to privacy are broadly drafted and therefore could apply to online matters (such as Article 378 as described above).

Additionally, as described in the 'Collection and Processing' section above, under certain circumstances, online privacy is

protected through Articles 21 and 22 of the Cyber Crime Law and the TRA's Consumer Protection Regulation. Unlawful access via the Internet, by electronic devices, of financial information (*eg,* Credit Cards and Bank Accounts) without permission is also an offense under the Cyber Crime Law (Articles 12 and 13).

KEY CONTACTS

Paul Allen
Head of Intellectual Property & Technology – Middle East
T +971 4 438 6295
paul.allen@dlapiper.com

Eamon Holley
Legal Director
T +971 4 438 6293
eamon.holley@dlapiper.com

Jamie Ryder
Senior Legal Consultant
T +971 4 438 6297
jamie.ryder@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UGANDA

Last modified 13 May 2019

LAW

Uganda recently enacted the Data Protection and Privacy Act, 2019 (Act) to supplement constitutional privacy protections under Article 27 of the Constitution of the Republic of Uganda. The Act regulates personal data collection, processing, use and disclosure, and applies to any person, entity or public body within or outside of Uganda who collects, processes, holds, or uses personal data. The Act will go into effect pending publication in the Uganda Gazette.

Sector specific laws further incorporate data protection provisions applicable to regulated activities, including:

- The Access to Information Act, 2005
- The Regulation of Interception of Communications Act, 2010
- The Computer Misuse Act, 2011
- The Registration of Persons Act, 2015

DEFINITIONS

Definition of Personal Data

Section 2 of the Act defines personal data as information about a person from which the person can be identified, such as information relating to nationality, age, marital status, education level, occupation and identity data.

This information is considered personal data regardless of the form in which the information is recorded.

Definition of Sensitive Personal Data

Section 9 of the Act defines "special personal data" as data relating to the religious or philosophical beliefs, political opinions, sexual life, financial information, health status or medical records of an individual.

NATIONAL DATA PROTECTION AUTHORITY

Section 4 of the Act establishes the National Information Technology Authority-Uganda as Uganda's personal data protection office. The office is not yet operational for data protection purposes.

REGISTRATION

Under Section 29 of the Act, the National Information Technology Authority-Uganda is authorized to maintain a data protection register of every person, institution or public body that collects or processes personal data, including the purpose of data collection or processing.

Registration requirements are not yet in effect, and are pending implementation regulations to be enacted by the Minister of

Information and Communications Technology.

DATA PROTECTION OFFICERS

Under Section 6 of the Act, covered entities are required to appoint a data protection officer responsible for ensuring compliance with the Data Protection and Privacy Act. The Act does not provide specific criteria for the appointment of data protection officers.

COLLECTION & PROCESSING

Restrictions on the collection or processing of the personal data

The Data Protection and Privacy Act restricts personal data collection and processing by:

- Requiring entities to obtain informed consent prior to personal data collection or processing
- Prohibiting the collection or processing of children's personal data unless: (i) done with the prior consent of a parent / guardian; (ii) necessary for compliance with the law; or (iii) for research or statistical purposes
- Prohibiting the collection or processing of special personal data unless specifically permitted by law
- Requiring that personal data be collected directly from the data subject, and only for a lawful or specific purpose related to the functions or activities of the data collector or controller
- Requiring data collectors, processors, and controllers to ensure that personal data is complete, accurate, up-to-date and not misleading
- Requiring that further processing of personal data be for a specific purpose related to the purpose for which personal data was collected
- Prohibiting personal data retention for a period longer than necessary to achieve the purpose for which data was collected and processed, unless specifically authorized by the Act, and
- Requiring destruction or de-identification of personal data records at the end of the retention period to prevent reconstruction of personal data in an intelligible form.

TRANSFER

Section 19 of the Data Protection and Privacy Act permits processing or storage of personal data outside Uganda if:

- Adequate measures are in place in the country in which the data is processed or stored, at least equivalent to protections under the Act, or
- With data subject consent.

SECURITY

Under Section 20 of the Act, data controllers, collectors and processors must secure the integrity of personal data in their control or possession by adopting appropriate measures to prevent loss and unauthorized destruction, processing or access to personal data.

Data controllers are specifically required to use measures that:

- Identify reasonable risks to personal data in their possession or control
- Establish and maintain appropriate precautions against the risks identified
- Regularly verify the effective implementation of the precautions, and
- Ensure that the safeguards are continually updated.

In instances where personal data is processed by third parties, entities must ensure that data processors apply security safeguards provided under the Act.

BREACH NOTIFICATION

Section 23 of the Data Protection and Privacy Act imposes a duty on data processors, collectors and controllers to immediately notify the National Information Technology Authority-Uganda of any reasonable belief that personal data has been accessed or acquired by an unauthorized person.

ENFORCEMENT

Remedial orders

The Act empowers the National Information Technology Authority-Uganda to enforce violations of the Act by issuing remedial orders and requiring compliance with data subject requests. Enforcement is generally triggered by complaints lodged with the Authority by aggrieved individuals or by data subjects seeking to enforce rights under the Act.

Compensation

Ugandan courts may award compensatory damages to persons harmed by data collector, controller or processor violations of the Act.

Sanctions

- Fines – Entities that violate the Act are subject to a fine of up to 245 currency points (UGX4.9 million). If an entity is a corporation, Ugandan courts may enforce violations of the Act by ordering a penalty of up to 2 percent of the corporation's annual gross turnover.

- Imprisonment – Ugandan courts may punish offenses under the Act with an imprisonment term of up to ten years. In addition to imprisonment, courts may order convicted offenders to pay a monetary fine.

ELECTRONIC MARKETING

There is no electronic marketing regulation in Uganda.

ONLINE PRIVACY

There is no specific online privacy regulation.

KEY CONTACTS

Sebalu & Lule Advocates
www.sebalulule.co.ug/

Barnabas Tumusingize
Managing Partner
Sebalu & Lule Advocates
T +256 213 250 013
brt@sebalulule.co.ug

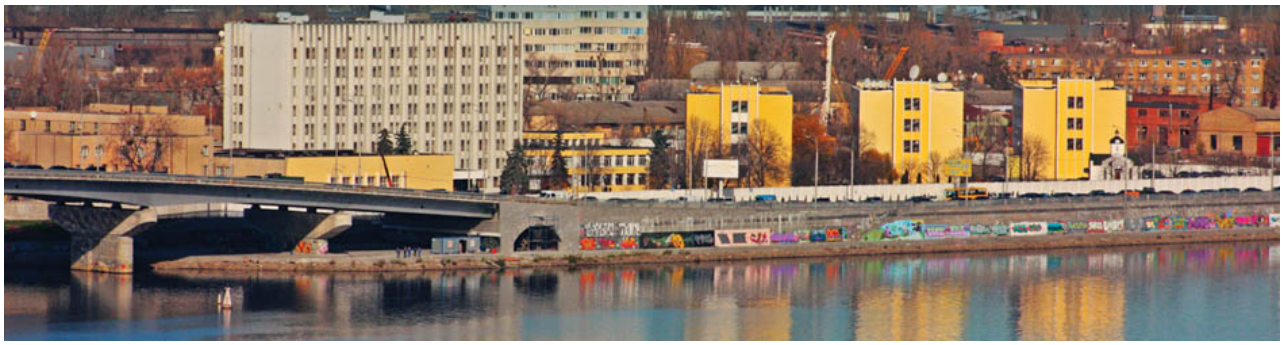
Paul Mbuga
Principal Associate
Sebalu & Lule Advocates
T +256 0312 2500013
mbuga@sebalulule.co.ug

Josephine Muhaise
Associate
Sebalu & Lule Advocates
T +256 414 233 063
jmuhaise@sebalulule.co.ug

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UKRAINE



Last modified 28 January 2019

LAW

The Law of Ukraine No. 2297 VI 'On Personal Data Protection' as of June 1, 2010 (Data Protection Law) is the main legislative act regulating personal data protection in Ukraine. On December 20, 2012, the Data Protection Law was substantially amended by the Law of Ukraine, 'On introducing amendments to the Law of Ukraine' 'On Personal Data Protection' dated November 20, 2012, No. 5491-VI. Additional significant changes to Data Protection Law were introduced by the Law of Ukraine 'On Amendments to Certain Laws of Ukraine regarding Improvement of Personal Data Protection System' dated July 3, 2013, No. 383-VII which came into force on January 1, 2014.

In addition to the Data Protection Law, certain data protection issues are regulated by subordinate legislation specifically developed to implement the Data Protection Law, in particular:

- Procedure of notification of the Ukrainian Parliament's Commissioner for Human Rights on the processing of personal data, which is of particular risk to the rights and freedoms of personal data subjects, on the structural unit or responsible person that organizes the work related to protection of personal data during processing thereof (Notification Procedure)
- Model Procedure of processing of personal data (Model Procedure)
- Procedure of control by the Ukrainian Parliament's Commissioner for Human Rights over the adherence of personal data protection legislation

The Data Protection Law essentially complies with EU Data Protection Directive 95/46/EC.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, executed in Strasbourg on January 28, 1981 and the Additional Protocol to the Convention regarding supervisory authorities and trans-border data flows, executed in Strasbourg on November 8, 2001 were ratified by the Ukrainian Parliament on July 6, 2010 (Convention on Automatic Processing of Personal Data) and have become fully effective in Ukraine.

In addition, data protection is regulated by:

- The Constitution of Ukraine dated June 28, 1996
- The Civil Code of Ukraine dated January 16, 2003, No 435 IV
- Law of Ukraine 'On Information' No 2657 XII, dated October 2, 1992
- Law of Ukraine 'On Protection of Information in the Information and Telecommunication Systems' dated July 5, 1994 No. 80/94 VR
- Law of Ukraine 'On Electronic Commerce' dated September 3, 2015, No 675-VIII
- Some other legislative acts

DEFINITIONS

Definition of personal data

Data Protection Law defines 'personal data' as data or an aggregation of data on an individual who is identified or can be precisely identified.

Definition of sensitive personal data

There is no definition of 'sensitive personal data'.

However, there is general prohibition to process personal data with regard to racial or ethnic origin, political, religious ideological convictions, participation in political parties and trade unions, accusation in criminal offenses or conviction to criminal punishment, as well as data relating to the health or sex life of an individual.

Processing of such data is allowed if unambiguous consent has been given by the personal data subject or based on exemptions envisaged by Data Protection Law *(eg,* the processing is performed for the reasons of protection of vital interest of individuals, healthcare purposes, in course of criminal proceedings, anti-terrorism purposes, etc.).

NATIONAL DATA PROTECTION AUTHORITY

Starting from January 1, 2014, Ukrainian Parliament's Commissioner for Human Rights (Ombudsman) is the state authority in charge of controlling the compliance of the data protection legislation.

REGISTRATION

As of January 1, 2014, the requirement of obligatory registration of personal data databases has been abolished. However, according to new wording of Data Protection Law, personal data owners are obliged to notify the Ombudsman about personal data processing which is of particular risk to the rights and freedoms of personal data subjects within 30 working days from commencement of such processing. Pursuant to the Notification Procedure, the following types of personal data processing requires obligatory notification to the Ombudsman:

- Racial, ethnic, national origin
- Political, religious ideological beliefs
- Participation in political parties and/or organizations, trade unions, religious organizations or civic organization of ideological direction
- State of health
- Sexual life
- Biometric data
- Genetic data
- Criminal or administrative liability
- Application of measures as part of pre-trial investigation
- Any investigative procedures relating to an individual
- Acts of certain types of violence used against an individual
- Location and / or route of an individual

The Notification Procedure envisages that the application for notification shall contain, inter alia the following information:

- Information about the owner of personal data
- Information about the processor(s) of personal data
- Information on the composition of personal data being processed
- The purpose of personal data processing
- Category(ies) of individuals whose personal data are being processed
- Information on third parties to whom the personal data are transferred
- Information on cross-border transfers of personal data
- Information on the place (address) of processing of personal data
- General description of technical and organizational measures taken by personal data owner in order to maintain the security of personal data

Where any of information listed above is submitted to the Ombudsman and has changed, the owner of the personal data shall notify the Ombudsman on such changes within 10 days from the occurrence of such change.

Additionally, the Notification Procedure requires the owners of personal data to notify the Ombudsman regarding the termination of personal data processing which is of particular risk to the rights and freedoms of personal data subjects, within ten days of such termination.

The Notification Procedure requires owners and processors of personal data that process personal data, which is of particular risk to the rights and freedoms of personal data subjects, to notify the Ombudsman on establishing a structural unit or appointing a person (data protection officer) responsible for the organization of work related to the protection of personal data during the processing. Such notification shall be made within 30 days of establishing a structural unit or appointing a responsible person.

Information regarding the said notifications of the Ombudsman shall be published on the official website of the Ombudsman.

DATA PROTECTION OFFICERS

Data owners and processors processing personal data that is of particular risk to the rights and freedoms of personal data subjects, must establish a special department or appoint a responsible person (data protection officer) to responsible for the personal data processing matters. Other owners and processors may either establish a department or appoint a responsible person on a voluntary basis.

There are no requirements for the data protection officer to be a citizen or a resident in Ukraine. However, if he or she is a foreign citizen under the general rule, a work permit must be obtained for him or her to hold such a position. There are no particular penalties for the incorrect appointment of Data Protection Officer.

COLLECTION & PROCESSING

The Data Protection Law requires obtaining the consent of data subjects for the processing of their personal data. According to the Data Protection Law, the consent of the data subject means the voluntary and intentional expression of will of the data subject to the processing of personal data for the identified purposes, expressed in writing or in some other form. In the area of e-commerce, consent may be granted in the process of registration of data subjects by "ticking" a consent box during registration, provided that such a system does not allow processing of personal data before the consent is obtained. Under certain circumstances, personal data may be processed without a data subject's consent (*eg*, legislative permission for processing of personal data, necessary to the conclusion and execution of a transaction or contract in favor of the data subject, protection of interests of data subject or data owner).

Pursuant to the Data Protection Law, as a general rule, personal data subjects shall be informed, at the moment of collection of their personal data of:

- The owner of their personal data
- The composition and content of their personal data being collected
- Their rights
- The purpose of their personal data collection, and
- The persons to whom their personal data will be transferred

However, in cases when the personal data of individuals have been collected based on the following grounds, the personal data subjects shall be informed of the above within 30 working days from the:

- Legislative permission of the owner of the personal data on the processing of personal data exclusively for the purposes of fulfilling its authorities
- Conclusion and execution of a transaction where the data subject is a party or the transaction has been concluded in favor of the data subject, which preceded conclusion of a transaction at the request of the subject of personal data
- Protection of vital interests of the data subject, or
- Need to protect the legitimate interests of the owner of personal data and third parties, except where a data subject requests that the processing of his/her personal data stops and the need to protect personal data prevails over such

interest

In addition, the Data Protection Law provides the data subject with the following rights:

- To be aware of the sources of collection, location of his / her personal data, the purpose of data processing, the address of the owner or processor of the personal data or to obtain the said information through his / her representatives
- To obtain information in regards to the conditions of providing access to personal data, and in particular, information on third parties, to which his / her personal data are transferred
- To access his / her personal data
- To obtain a reply within 30 calendar days from the date of the receipt of his / her request, informing the individual whether his / her personal data is being processed and to receive the contents of such personal data
- To provide the owner of personal data with the reasonable request to terminate the processing of his / her personal data
- To provide a reasonable request to change or destroy his / her personal data by any owner and processor of the personal data if the data is processed illegally or is inaccurate
- To protect of his / her personal data from unauthorized processing and accidental loss, elimination or damage with respect to intended encapsulation, not providing or the untimely provision of personal data, and to protect from providing invalid or discrediting information regarding the individual
- To appeal violations in the course of personal data processing to the Ombudsman or to the court
- To introduce limitations as regards rights on its personal data processing while giving the consent
- To use the means of legal protection in the case of violation of rights to personal data
- To revoke its consent on personal data processing
- To be aware of the mechanism of automatic personal data processing, and
- To be protected from the automated decision that has legal effects

The owner of the personal data can entrust the processing of personal data to the processor pursuant to a written agreement requiring that the processor process the personal data only for the purposes and in the amount permitted under the agreement. The transfer of personal data to the processor is permitted only with consent of the data subject.

TRANSFER

In accordance with Data Protection Law, personal data may be transferred to foreign parties when there is an appropriate level of protection of personal data in the respective state of the transferee. Pursuant to the Data Protection Law, such states include member states of the European Economic Area and signatories to the EC Convention on Automatic Processing of Personal Data. The list of the states ensuring an appropriate level of protection of personal data will be determined by the Cabinet of Ministers of Ukraine.

Personal data may be transferred abroad based on one of the following grounds:

- Unambiguous consent of the personal data subject
- Cross-border transfer is needed to enter into or perform a contract between the personal data owner and a third party in favor of the data subject
- Necessity to protect the vital interests of the data subject
- Necessity to protect public interest, establishing, fulfilling and enforcing of a legal requirement
- Non-interference in personal and family life of the data subject, as guaranteed by the data owner

SECURITY

The data owners and processors must take appropriate technical and organizational measures to ensure the protection of personal data against unlawful processing, including against loss, unlawful or accidental elimination, and also against unauthorized access. In this regard, owners and processors processing personal data which is of particular risk to the rights and freedoms of personal data subjects shall determine a special department or a responsible person to organize the work related to the protection of personal data during the processing thereof (other owners and processors may either establish a department or appoint a responsible person on a voluntary basis).

The Model Procedure stipulates that the owners and processors of personal data shall take measures to maintain the security of

personal data in all stages of their processing, including organizational and technical measures for the protection of personal data. Organizational measures shall include:

- Determination of a procedure of access to personal data by employees of the owner / processor of personal data
- Determination of the order of the recording of operations related to the processing of personal data o and access to them
- Elaboration of an action plan in case of unauthorized access to personal data, damage of technical equipment or occurrence of emergency situations, and
- Regular trainings of employees working with personal data

Personal data, irrespective of the manner of its storage, shall be processed in the way which makes unauthorized access to the data by third persons impossible.

With the purpose of maintenance of security of personal data, technical security measures shall be taken which would exclude the possibility of unauthorized access to personal data being processed and ensure the proper work of technical and program complex through which the processing of personal data is performed.

Additionally, the Data Protection Law requires establishing a structural unit or appointing a responsible person within the personal data owners / processors processing the personal data which is of particular risk to the rights and freedoms of personal data subjects. Such structural unit or responsible person shall organize the work related to protection of personal data during the processing thereof.

BREACH NOTIFICATION

There is no requirement to report data security breaches or losses to the appropriate state authority.

ENFORCEMENT

According to Data Protection Law, the Ombudsman and Ukrainian courts are responsible for overseeing the compliance of personal data protection legislation. Failure to comply with the provisions of Data Protection Law can lead to the penalties prescribed by the law.

Violation of personal data protection legislation may result in civil, criminal and administrative liability.

If the violation has led to material or moral damages, the violator may be required by the court to reimburse such damages.

The Code of Ukraine on Administrative Offenses envisages administrative liability for the following breaches of Ukrainian data protection legislation:

- Failure to notify or delay in providing notification to the Ombudsman regarding the processing of personal data or of a change to the information submitted, subject to notification requirements under Ukrainian legislation, or submission of incomplete or false information, which may lead to a fine of up to €214
- Non-fulfilment of legitimate requests (orders) from the Ombudsman or determined state officials of the Ombudsman's secretariat, regarding the elimination or prevention of violations of personal data protection legislation, which may lead to a fine of up to €535
- Non-fulfillment of legitimate requests of Ombudsman or its representatives, which may lead to a fine of up to €107
- Non-observance of the established procedure for the protection of personal data which leads to the unauthorized access of the personal data or violation of rights of the data subject, which may lead to a fine of up to €535

The criminal liability, prescribed by the Criminal Code of Ukraine, envisages fines of up to €491 or correctional works for a term of up to two years, up to six months arrest, or up to three years of limitation of freedom for the illegal collection, storing, use, elimination, or spreading of confidential information about an individual, or an illegal change of such information.

ELECTRONIC MARKETING

The Law of Ukraine 'On Electronic Commerce' dated September 3, 2015 provides for certain legal requirements for distribution

of commercial electronic messages in the area of electronic commerce. In particular, commercial electronic messages shall be distributed only subject to the consent given by individual to whom such messages are addressed. At the same time, commercial electronic messages may be distributed to an individual without his / her consent only if such individual has an option to object to receiving such messages in future.

In addition, commercial electronic messages shall satisfy the following criteria:

- Commercial electronic messages shall unequivocally be identified as such.
- The recipient shall have easy access to information regarding the person sending the message as stipulated by the Law of Ukraine 'On Electronic Commerce', in particular: (i) full name of legal entity / individual and place of registration / residence; (ii) email / website of the online shop; (iii) registration number or tax ID number / passport details (for individuals); (iv) license data (in case if it is mandatory under the law); (v) inclusion of taxes in calculation of the price of goods / services; and (vi) price of delivery of goods (in case if delivery is performed).
- Commercial electronic messages regarding sales, promotional gifts, premiums and etc. shall be unequivocally identified as such and the conditions of receiving of such promotions shall be clearly stated to avoid their ambiguous understanding as well as shall comply with advertising legislation.

ONLINE PRIVACY

There is no specific legislation regulating online privacy in Ukraine. However, the Data Protection Law applies to the extent online activities involve the processing of personal data.

KEY CONTACTS

Natalia Pakhomovska
Partner
T +380 44 495 1789
natalia.pakhomovska@dlapiper.com

Natalia Kirichenko
Legal Director
T +380 44 490 9575
natalia.kirichenko@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UNITED KINGDOM

Last modified 24 May 2018

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The GDPR will come into force in the United Kingdom on 25 May 2018, on which date the UK will continue to be a Member State of the European Union.

Alongside the GDPR, the United Kingdom has prepared a new national data protection law, the Data Protection Act 2018 ("DPA"), which also comes into force on 25 May 2018. As well as containing derogations and exemptions from the position under the GDPR in certain permitted areas, the DPA also does the following:

- allows for the continued application of the GDPR in UK national law once the UK leaves the European Union (expected to be 29 March 2019);
- Part 3 of the DPA transposes the Law Enforcement Directive ((EU) 2016/680) into UK law, creating a data protection regime specifically for law enforcement personal data processing;
- Part 4 of the DPA updates the data protection regime for national security processing; and
- Parts 5 and 6 set out the scope of the Information Commissioner's mandate and her enforcement powers, and creates a number of criminal offences relating to personal data processing.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using "*all means reasonably likely to be used*" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

"Public authority" and "public body" are expressions used in the GDPR. For the purposes of the UK, the DPA defines them by reference to the definition of "public authority" used in the Freedom of Information Act 2000.

The DPA also clarifies that, where the purpose and means of processing are determined by an enactment of law, then the person on whom the obligation to process the data is imposed by the enactment is the controller.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Information Commissioner (whose functions are discharged through the Information Commissioner's Office ("ICO")) is the supervisory authority for the UK for the purposes of art. 51 of the GDPR.

The ICO's contact details are:

Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
T +0303 123 1113 (or +44 1625 545745 if calling from overseas)
F 01625 524510
www.ico.org.uk

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

In accordance with the position advocated by recital 89 of the GDPR, the UK's system of general registration for controllers will be abolished from 25 May 2018.

However, the UK has opted to replace the system of general registration with a fee-paying scheme for controllers, known as the Data Protection Fee. Controllers will have to pay an annual data protection fee to the ICO, unless they are exempt from doing so.

Those controllers who have an unexpired registration under the old system will not be required to pay the new fee until their existing registration expires, at which point the ICO will contact them with details of the new fee.

Parliament has set the fees based on its perception of the risks posed by controllers processing personal data. The amount payable depends upon staff numbers and annual turnover or whether the controller is a public authority, a charity or a small occupational pension scheme. Not every controller must pay a fee – there are exemptions. The maximum fee, for large organisations, is £2,900.

The maximum penalty for a controller who breaks the law by not paying a fee (or not paying the correct fee) is a fine of £4,350 (150% of the top tier fee).

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The UK has not opted to extend the requirement to appoint a Data Protection Officer.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organisations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose

- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Special categories of personal data (Article 9)

Article 9(2) of the GDPR provides for a number of exceptions under which special categories of personal data may lawfully be processed. Certain of these exceptions require a basis in Member State law. Parts 1 and 2 of Schedule 1 to the DPA provide a number of such bases, in the form of 'conditions', which in effect provide UK specific gateways to legalise the processing of certain types of special category data. Many of these conditions are familiar from the previous UK law, whilst other are new. Important examples include:

- processing required for employment law;
- heath and social care;

- equal opportunity monitoring;
- public interest journalism;
- fraud prevention;
- preventing / detecting unlawful acts (eg money laundering / terrorist financing);
- insurance; and
- occupational pensions.

Criminal convictions and offences data (Article 10)

The processing of criminal conviction or offences data is prohibited by Article 10 of the GDPR, except where specifically authorised under relevant member state law. Part 3 of Schedule 1 of the DPA authorises a controller to process criminal conviction or offences data where the processing is necessary for a purpose which meets one of the conditions in Parts 2 of Schedule 1 (this covers the conditions noted above other than processing for employment law, health and social care), as well as number of other specific conditions:

- consent;
- the protection of a data subject's vital interests; and
- the establishment, exercising or defence of legal rights, the obtaining of legal advice and the conduct of legal proceedings

Appropriate policy and additional safeguards

In any case where a controller wishes to rely on one of the DPA conditions to lawfully process special category, criminal conviction or offences data, the DPA imposes a separate requirement to have an appropriate policy document in place and apply additional safeguards to justify the processing activity. The purpose of the policy document is to set out how the controller intends to comply with each of the data protection principles in Article 5 of the GDPR in relation to this more sensitive processing data activity.

Child's consent to information society services (Article 8)

Article 8(1) of the GDPR stipulates that a child may only provide their own consent to processing in respect of information society (primarily, online) services, where that child is over 16 years of age, unless member state law applies a lower age. The DPA reduces the age of consent for these purposes to 13 years for the UK.

Automated Decision Making (Article 22)

Article 22(2)(b) of the GDPR allows member states to authorise automated decision making in local law, subject to additional safeguards, for purposes beyond the two permitted gateways already set out in Article 22(2) of the GDPR (ie, explicit consent, or necessity for entering into or performance of a contract with the data controller).

The DPA takes advantage of this provision to enable automated decision making where the automated decision is accompanied by the sending of a specific notice to the data subject which provides them with a one month period to request the controller to (i) reconsider the decision, or (ii) take a new decision that is not based solely on automated processing.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions),

Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU - U.S. Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

Once the UK leaves the EU (expected to be the 29 March 2019) it will become a third country for the purposes of Chapter V of the GDPR. It is possible that the UK will achieve an adequacy decision to coincide with its date of exit (such a decision would not be surprising, given the UK's desire to continue applying the GDPR). However, in the absence of an adequacy decision, alternative safeguards would technically be required to transfer personal data from the EU to the UK. This area remains uncertain, and it is recommended that organisations closely monitor the unfolding picture in respect of the UK / EU negotiations

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Personal data breaches should be notified to the ICO, as the UK's supervisory authority. Breaches can be reported to the ICO's dedicated breach helpline during office hours (+44 303 123 1113). Outside of these hours (or where a written notification is is preferred) a pro forma may be downloaded and emailed to the ICO.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;

- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The DPA sets out the specific enforcement powers provided to the ICO pursuant to Article 58 of the GDPR, including:

- information notices - requiring the controller or processor to provide the ICO with information;
- assessment notices - permitting the ICO to carry out an assessment of compliance;
- enforcement notices - requiring the controller or processor to take, or refrain from taking, certain steps; and
- penalty notices - administrative fines.

The ICO has the power to conduct a consensual audit of a controller or a processor, to assess whether that organisation is complying with good practice in respect of its processing of personal data.

Under Schedule 15 of the DPA, the ICO also has powers of entry and inspection. These will be exercised pursuant to judicial warrant and will allow the ICO to enter premises and seize materials.

The DPA creates two new criminal offences in UK law: the re-identification of de-identified personal data without the consent of the controller and the alteration of personal data to prevent disclosure following a subject access request under Article 15 of the GDPR. The DPA retains existing UK criminal law offences, eg offence of unlawfully obtaining

personal data.

The DPA requires the ICO to issue guidance on its approach to enforcement, including guidance about the circumstances in which it would consider it appropriate to issue a penalty notice, i.e. administrative fine.

The DPA also requires the ICO to publish statutory codes of practice on direct marketing and data sharing (preserving the position under the previous law).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation, a change which is currently forecast for Spring 2019. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (eg an email address is likely to be 'personal data' for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to prevent the processing of their personal data (eg a right to 'opt-out') for direct marketing purposes.

There are a number of different opt-out schemes/preference registers for different media types. Individuals (and, in some cases, corporate subscribers) can contact these schemes and ask to be registered as not wishing to receive direct marketing material. If advertising materials are sent to a person on the list, sanctions can be levied by the ICO using his powers under the Act.

The PEC Regulations prohibit the use of automated calling systems without the consent of the recipient. The PEC Regulations also prohibit unsolicited electronic communications (ie by email or SMS text) for direct marketing purposes without prior consent from the consumer unless:

- the consumer has provided their relevant contact details in the course of purchasing a product or service from the person proposing to undertake the marketing
- the marketing relates to offering a similar product or service, and
- the consumer was given a means to readily 'opt out' of use for direct marketing purposes both at the original point where their details were collected and in each subsequent marketing communication.

Each direct marketing communication must not disguise or conceal the identity of the sender and include the 'unsubscribe' feature referred to above.

The restrictions on marketing by email / SMS only applies in relation to individuals and not where marketing to corporate subscribers.

ONLINE PRIVACY

The PEC Regulations (as amended) deal with the collection of location and traffic data by public electronic communications services providers ('CSPs') and use of cookies (and similar technologies).

Traffic Data

Traffic Data held by a CSP must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication.

However, Traffic Data can be retained if:

- it is being used to provide a value added service, and
- consent has been given for the retention of the Traffic Data.

Traffic Data can also be processed by a CSP to the extent necessary for:

- the management of billing or traffic
- dealing with customer enquiries
- the prevention of fraud, or
- the provision of a value added service.

Cookie Compliance

The use and storage of cookies and similar technologies requires:

- clear and comprehensive information, and
- consent of the website user.

The ICO has confirmed that consent can be implied where a user proceeds to use a site after being provided with clear notice (eg by way of a pop-up or banner) that use of site will involve installation of a cookie.

Consent is not required for cookies that are:

- used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or
- strictly necessary for the provision of a service requested by the user.

Enforcement of a breach of the PEC Regulations is dealt with by the ICO and sanctions for breach are the same as set out in the enforcement section above.

KEY CONTACTS

Andrew Dyson
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +44 (0)113 369 2403
andrew.dyson@dlapiper.com

Ross McKean
Partner
T +44 (0) 20 7796 6077
ross.mckean@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UNITED STATES

Last modified 28 January 2019

LAW

The US has several sector-specific and medium-specific national privacy or data security laws, including laws and regulations that apply to financial institutions, telecommunications companies, personal health information, credit report information, children's information, telemarketing and direct marketing.

The US also has hundreds of privacy and data security among its 50 states and territories, such as requirements for safeguarding data, disposal of data, privacy policies, appropriate use of Social Security numbers and data breach notification. California alone has more than 25 state privacy and data security laws, including the recently enacted California Consumer Privacy Act of 2018 (CCPA), effective January 1, 2020. The CCPA applies cross-sector and introduces sweeping definitions and broad individual rights, and imposes substantial requirements and restrictions on the collection, use and disclosure of personal information, which is very broadly defined as explained below.

In addition, the US Federal Trade Commission (FTC) has jurisdiction over a wide range of commercial entities under its authority to prevent and protect consumers against unfair or deceptive trade practices, including materially unfair privacy and data security practices. The FTC uses this authority to, among other things, issue regulations, enforce certain privacy laws and take enforcement actions and investigate companies for:

- Failing to implement reasonable data security measures
- Making materially inaccurate privacy and security representations including in privacy policies
- Failing to abide by applicable industry self-regulatory principles
- Transferring or attempting to transfer personal information to an acquiring entity in a bankruptcy or M&A transaction, in a manner not expressly disclosed on the applicable consumer privacy policy
- Violating consumer privacy rights by collecting, using, sharing or failing to adequately protect consumer information, in violation of the FTC's consumer privacy framework or certain national privacy laws and regulations

Many state attorneys general have similar enforcement authority over unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states.

As illustrated above, US privacy law is a complex patchwork of national privacy laws and regulations that address particular issues or sectors, state laws that further address privacy and security of personal information, and federal and state prohibitions against unfair or deceptive business practices. While this chapter provides an overview of US national and state privacy and security laws and highlights key aspects of such laws, these laws are too diverse to summarize fully. Further, US privacy law is currently in flux—in 2019, the California Attorney General will be issuing CCPA regulations and several other states are expected to pass significant privacy laws. While support is growing for a comprehensive, national privacy law that would supersede and preempt state privacy laws, it is unlikely such a law will be adopted in 2019.

DEFINITIONS

Definition of personal data

Varies widely by regulation. The FTC now considers information that is linked or reasonably linkable to a specific individual, which could include IP addresses and device identifiers, as personal data.

The CCPA defines personal information as any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The definition specifically includes contact information, government IDs, biometrics, genetic data, location data, account numbers, education history, purchase history, online and device IDs, and search and browsing history and other online activities, if such information is linked or linkable with a particular consumer or household. Under the law, consumer is broadly defined as any resident of California.

In contrast, state breach notification laws and data security laws typically define personal information more narrowly focusing on more sensitive categories of information, as described below.

Definition of sensitive personal data

Varies widely by sector and by type of statute.

Generally, personal health data, financial data, credit worthiness data, student data, biometric data, personal information collected online from children under 13, and information that can be used to carry out identity theft or fraud are considered sensitive.

For example, state breach notification laws and data security laws generally apply to more sensitive categories of information, such as Social security numbers and other government identifiers, credit card and financial account numbers, health or medical information, insurance ID, online account credentials, digital signatures, and/or biometrics.

NATIONAL DATA PROTECTION AUTHORITY

No single national authority.

The FTC has jurisdiction over most commercial entities and has authority to issue and enforce privacy regulations in specific areas (eg, for telemarketing, commercial email, and children's privacy) and to take enforcement action to protect consumers against unfair or deceptive trade practices, including materially unfair privacy and data security practices.

Many state attorneys general have similar enforcement authority over unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states.

In addition, a wide range of sector-specific regulators, particularly those in the healthcare, financial services, telecommunications and insurance sectors, have authority to issue and enforce privacy and security regulations, with respect to entities under their jurisdiction.

REGISTRATION

There is no requirement to register databases or personal information processing activities.

In 2018, Vermont passed legislation requiring data brokers to register with the secretary of state and adhere to minimum data security standards. Under the law a “data broker” is defined as a company that collects computerized, personal information of Vermont residents with whom the company has no direct relationship, and eithers sell or licenses that information.

In addition, several state laws require entities that engage in certain types of telemarketing activities to register with the state attorney general or other consumer protection agency.

DATA PROTECTION OFFICERS

With the exception of entities regulated by HIPAA, there is no general requirement to appoint a formal data security officer or data privacy officer.

Massachusetts and some other state laws and federal regulations require organizations to appoint one or more employees to maintain their information security program.

Even so, appointing a chief privacy officer and a chief information security officer is a best practice which is common among larger organizations and increasingly also among mid-sized ones.

COLLECTION & PROCESSING

US privacy laws and self-regulatory principles vary widely, but generally require pre-collection notice *(eg,* in a privacy policy) of information collection, use and disclosure practices, related consumer choices and company contact information, as well as an opt-out for marketing uses or disclosures of personal information.

Opt-in consent is generally required when personal information that is considered sensitive under US law is collected, used, and shared, such as health information, credit reports, financial information, student data, children's personal information, biometric data, video viewing choices, geolocation data and telecommunication usage information.

Further, companies generally need to obtain opt-in consent prior to using, disclosing or otherwise treating personal information in a manner that is materially different than what was disclosed in the privacy policy applicable when the personal information was collected. The FTC deems such changes 'retroactive material changes' and considers it unfair and deceptive to implement a retroactive material change without obtaining prior, affirmative consent from all relevant individuals.

Under the CCPA (which applies to individual and household data about California residents and takes effect January 1, 2020), businesses must, among other things:

- At or before collection, notify individuals of the categories of personal information to be collected and the purposes of use of such information
- Post a privacy policy that discloses categories of personal information collected, purposes of use, categories of service providers and other third parties to whom information is disclosed or sold, and individual rights *(eg,* access, deletion, data portability) and how to exercise them, as well as other minimum requirements
- A "do-not-sell my information" link and page where consumers can opt-out of the sale of their personal information (if applicable)
- Other California privacy laws (*eg*, the California "Shine the Light Law" and the California Online Privacy Protection Act) currently in force impose additional notice obligations, including:
- Where any personal information is disclosed to a third party for their own marketing use, a specific notice about such disclosure (*eg*, in a company's privacy policy) must be provided and accessible through a special link on their homepage. Further, the law gives California residents to request a list of the personal information and third parties to whom such information was disclosed for marketing purposes in the prior 12 months
- Whether the company honors any do-not-track mechanisms

Other states impose a wide range of specific requirements, particularly in the student and employee privacy areas. For example, a significant number of states have enacted employee social media privacy laws, and, in 2014 and 2015, a disparate array of education privacy laws. In addition, there a number of sector-specific privacy laws that impose notice obligations, significantly limit permitted disclosures of personal information, and grant individuals the right to access or review records about the individual that are held by the regulated entity.

The US also regulates marketing communications extensively, including telemarketing, text message marketing, fax marketing and email marketing (which is discussed below).

Under the CCPA, prior to any sale of personal information, companies must provide individuals over 16 years old the right to opt-out, obtain prior consent from individuals ages 13 to 16, and obtain prior parental consent from individuals younger than 13. Sale is broadly defined to include selling, disclosing or granting access to personal information in exchange for any consideration or other thing of value. The CCPA also gives individuals broad access and data portability rights, as well as limited deletion rights and the right to obtain more detailed information about specific data collected, as well as disclosures of personal data by businesses.

TRANSFER

No geographic transfer restrictions apply in the US, except with regard to storing some government information.

The US is a major point of storage of personal data. The US is presently considered an "adequate" destination for transfers of personal from the EU and Switzerland to recipients in the US who are certified to the EU-US and Swiss-US Privacy Shield principles and program, respectively. However, the legality of the EU-US Privacy Shield program is being challenged in a case that will eventually be heard by the Court of Justice of the European Union.

SECURITY

Most US businesses are required to take reasonable technical, physical and organizational measures to protect the security of sensitive personal information (*eg,* health or financial information, telecommunications usage information, biometric data, or information that would require security breach notification). A few states have enacted laws imposing more specific security requirements for such data. For example, Massachusetts has enacted regulations that apply to any company that collects or maintains sensitive personal information (*eg,* name in combination with Social Security number, driver's license, passport number, or credit card or financial account number) on Massachusetts residents. Among other things, the Massachusetts regulations require regulated entities to have a comprehensive, written information security program and set forth the minimum components of such program, including binding all service providers who touch this sensitive personal information data to protect it in accordance with the regulations. Massachusetts law includes encryption requirements on the transmission of sensitive personal information across wireless networks or beyond the logical or physical controls of an organization, as well as on sensitive personal data stored on laptops and portable storage devices. Some states impose further security requirements on payment card data and other sensitive personal information.

There are also a number of other sectoral data security laws and regulations that impose specific security requirements on regulated entities – such as in the financial, insurance and health sectors. Federal financial regulators impose extensive security requirements on the financial services sector, including requirements for security audits of all service providers who receive data from financial institutions. For example, the New York Department of Financial Services (NYDFS) regulations impose extensive cybersecurity and data security requirements on licensees of the NYDFS, which includes financial services and insurance companies. The national Gramm-Leach-Bliley Act and implementing regulations require financial institutions to implement reasonable security measures.

HIPAA regulated entities are subject to much more extensive data security requirements. HIPAA security regulations apply to so-called 'covered entities' such as doctors, hospitals, insurers, pharmacies and other healthcare providers, as well as their 'business associates' which include service providers who have access to, process, store or maintain any protected health information on behalf of a covered entity. 'Protected health information' under HIPAA generally includes any personally identifiable information collected by or on behalf of the covered entity during the course of providing its services to individuals.

Internet of Things

California recently enacted the first US Internet of Things (IoT) legislation, effective January 1, 2020. Under SB 327, manufacturers of most IoT and Bluetooth connected devices will be required to implement reasonable security features 'appropriate to the nature and the function of the device and the information the device may collect, contain or transmit' and 'designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.'

BREACH NOTIFICATION

All 50 US states, Washington, DC, and most US territories (including, Puerto Rico, Guam and the Virgin Islands) have passed breach notification laws that require notifying state residents of a security breach involving more sensitive categories of information, such as Social Security numbers and other government identifiers, credit card and financial account numbers, health or medical information, insurance ID, tax ID, birthdate, as well as online account credentials, digital signatures and/or biometrics.

Under many state laws, where more than 500 individuals are impacted, notice is must also be provided to credit bureaus. Nearly half of states also require notice to state attorneys general and / or other state officials of certain data breaches. Also, some state data breach laws impose certain (varying) notice content and timing requirements with respect to notice to individuals and to state attorneys general and/or other state officials.

Federal laws require notification in the case of breaches of healthcare information, breaches of information from financial institutions, breaches of telecom usage information held by telecommunication providers, and breaches of government agency information.

ENFORCEMENT

Various entities enforce US national and state privacy laws. In addition, individuals may bring private rights of action (and class actions) for certain privacy or security violations.

Violations are generally enforced by the FTC, state attorneys general or the regulator for the industry sector in question. Civil penalties can be significant.

In addition, some privacy laws (for example, credit reporting, marketing and electronic communications, video viewing history, call recording and cable communications privacy laws) may be enforced through private rights of action, which give rise to class action lawsuits for significant statutory damages and attorney's fees, and individuals may bring actions for actual damages from data breaches.

The CCPA (effective January 1, 2020) also authorizes individuals to take a private right of action for statutory damages of between US$100 and US$750 per individual for data breaches resulting from a business's failure to implement reasonable data security procedures (this applies to most categories of personal information under California's breach notification law) – this raises significant class action risks.

In June 2018, Ohio became the first US state to pass cybersecurity safe harbor legislation. Under SB 220, a company that has suffered a data breach of personal information has an affirmative defense if it has 'created, maintained, and complied with a written cybersecurity program that contains administrative, technical, and physical safeguards to protect personal information that reasonably conforms to an industry recognized cybersecurity framework' (*eg*, PCI-DSS standards, NIST Framework, NIST special publications 800-171, 800-53, and 800-53a, FedRAMP security assessment framework, HIPAA, GLBA).

ELECTRONIC MARKETING

The US regulates marketing communications extensively, including email and text message marketing, as well as telemarketing and fax marketing.

Email

The CAN-SPAM Act is a federal law that applies labeling and opt-out requirements to all commercial email messages. CAN-SPAM generally allows a company to send commercial emails to any recipient, provided the recipient has not opted out of receiving such emails from the sender, the email identifies the sender and the sender's contact information, and the email contains instructions on how the recipient can easily and without cost opt out of future commercial emails from the sender. The FTC and state attorneys general, as well as ISPs and corporate email systems can sue violators. Knowingly falsifying the origin or routing of a commercial email message is a federal crime.

Text Messages

Federal and state regulations apply to the sending of marketing text messages to individuals. Express consent is required to send text messages to individuals, and, for marketing text messages, express written consent is required (electronic written consent is sufficient, but verbal consent is not). The applicable regulations also specify the form of consent. This is a significant class action risk area, and any text messaging (marketing or informational) program needs to be carefully reviewed for strict compliance with legal requirements.

Calls to Wireless Phone Numbers

Similar to text messages, federal and state regulations apply to marketing calls to wireless phone numbers. Prior express consent is required to place phone calls to wireless numbers using any autodialing equipment, and, for marketing calls, express written consent is required (electronic written consent is sufficient, but verbal consent is not). The applicable regulations also specify the

form of consent. This is a significant class action risk area, and any campaign or program that involves calls (marketing or informational) to phone numbers that may be wireless phone numbers needs to be carefully reviewed for strict compliance with legal requirements. The definition of autodialing equipment is generally considered to, broadly, include any telephone system that is capable of (whether or not used or configured storing or producing telephone numbers to be called, using a random or sequential number generator.

Telemarketing

Beyond the rules applicable to text messaging and calling to wireless phone numbers, there are federal and state telemarketing laws as well. Federal telemarketing laws apply to most telemarketing calls and programs, and state telemarketing law will apply to telemarketing calls placed to or from within that particular state. As a result, most telemarketing calls are governed by federal law, as well as the law of one or more states. Telemarketing rules vary by state, and address many different aspects of telemarketing, such as calling time restrictions, do-not-call registries, opt-out requests, mandatory disclosures, requirements for completing a sale, executing a contract or collecting payment during the call, further restrictions on the use of auto-dialers and pre-recorded messages, and record-keeping requirements. Many states also require telemarketers to register or obtain a license to place telemarketing calls.

Fax Marketing

Federal law and regulations generally prohibit the sending of unsolicited advertising by fax without prior, express consent. Violations of the law are subject to civil actions and have been the subject of numerous class action lawsuits. The law exempts faxes to recipients that have an established business relationship with the company on whose behalf the fax is sent, as long as the recipient has not opted out of receiving fax advertisements and has provided their fax number 'voluntarily,' a concept which the law specifically defines.

The law also requires that each fax advertisement contain specific information, including:

- A 'clear and conspicuous' opt-out method on the first page of the fax
- A statement that the recipient may make a request to the sender not to send any future faxes and that failure to comply with the request within 30 days is unlawful, and
- A telephone number, fax number, and cost-free mechanism to opt-out of faxes, which permit consumers to make opt-out requests 24 hours a day, seven days a week
- Violations are subject to a private right of action and statutory damages, and thus pose a risk of class action lawsuits

ONLINE PRIVACY

There is no specific federal law that *per se* regulates the use of cookies, web beacons and other similar tracking mechanisms. However, the state online privacy laws require notice of online tracking and of how to opt out of it.

Under California law, any company that tracks any personally identifiable information about consumers over time and across multiple websites must disclose in its privacy policy whether the company honors any 'Do-Not-Track' method or provides users a way to opt out of such tracking; however, the law does not mandate that companies provide consumers a 'Do-Not-Track' option. The same law also requires website operators to disclose in their privacy policy whether any third parties may collect any personally identifiable information about consumers on their website and across other third party websites, and prohibits the advertising of certain products, services and materials (including alcohol, tobacco, firearms, certain dietary supplements, ultraviolet tanning, tattoos, obscene matters, etc.). Further, given the CCPA's broad definition of personal information, information collected via cookies, online, mobile and targeted ads, and other online tracking are likely to be subject to the requirements of the law.

It is best practice for websites that allow behavioral advertising on their websites to participate in the Digital Advertising Alliance industry self-regulatory principles, which including principles for online behavioral advertising (OBA Principles), which includes principles of transparency and choice – users must be able to opt out of being tracked for behavioral advertising purposes. The DAA is expected to update its OBA Principles in light of the CCPA.

Minors

The Children's Online Privacy Protection Act and regulations (COPPA) applies to information collected automatically (*eg*, via cookies) from child-directed websites and online services and other websites, online services and third party ad networks or plug-ins that knowingly collect personal information online from children under 13. COPPA also regulates behavioral advertising to children under 13 as well as the collection of geolocation information, requiring prior verifiable parental consent to engage in such advertising or collection.

California law requires that operators of websites or online services that are directed to minors or that knowingly collect personally identifiable information from minors permit minors that are registered users of their sites to remove any content the minor has posted from the site or online service. The law does not give minors the right to remove information posted by third parties. Minors must be given clear notice on how to exercise their right to removal.

Location Data

Generally, specific notice and consent in needed to collect precise *(eg,* mobile device) location information.

KEY CONTACTS

Jim Halpert
Partner & Chair of US Data Protection and Privacy Group
T +1 202 799 4441
jim.halpert@dlapiper.com

Jennifer Kashatus
Partner, Data Protection, Privacy and Security
T +1 202 799 4448
jennifer.kashatus@dlapiper.com

Kate Lucente
Partner and Co-Editor, Data Protection Laws of World Handbook
T +1 813 222 5927
kate.lucente@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

URUGUAY

Last modified 28 January 2019

LAW

Data Protection Act Law No. 18.331 (August 11, 2008); Decree No. 414/009 (August 31, 2009) (the Act).

DEFINITIONS

Definition of personal data

Any kind of information related to an identified or identifiable person or legal entity.

Definition of sensitive personal data

Any kind of personal data evidencing: racial or ethnic origin, political preferences, religious or moral beliefs, trade union membership or any kind of information concerning health or sexual life.

NATIONAL DATA PROTECTION AUTHORITY

Unidad Reguladora y de Control de Datos Personales (URCDP or Data Protection Authority).

REGISTRATION

Every database must be registered with the Data Protection Authority in Uruguay if the data processing is performed by a person located within the Uruguayan territory. When the person responsible for the data processing is located abroad, the database must be registered in Uruguay if: (i) such processing activities occur in connection with goods / services offered to Uruguayan people, (ii) it is required by any contract or other international laws, or (iii) the data is processed by means located in Uruguay.

The database must be registered by filing mandatory forms, which must be signed by a representative of the company that owns the database.

DATA PROTECTION OFFICERS

Certain entities are required to appoint a data protection officer (in Spanish, *"delegado de protección de datos"*). This obligation is imposed on public entities, private entities owned by the government and private entities whose core activity is the processing of sensitive data or large amounts of data.

The data protection officer is responsible for (a) formulating, designing and implementing data protection policies, (b) monitoring the compliance with local legislation and regulation, and (c) serving as a link to the Data Protection Authority.

COLLECTION & PROCESSING

In order to collect personal data contained in a database, the data processor must first obtain prior, documented consent from the individual or entity whose information is being processed. Documented consent is not required in the following cases:

- Personal data obtained from public sources
- Personal data obtained by public bodies to comply with legal obligations
- Personal data limited to domicile address, telephone number, ID number, nationality, tax number, corporation name
- Personal data obtained based on a contractual or professional relationship, which is necessary to perform the contract or the development of the professional services to be rendered, or
- Personal data obtained by individuals or corporations for their personal and exclusive use

The personal data processed cannot be used for purposes, different from those that justified the initial acquisition of the information. There must be legitimate reasons (*ie*, reasons which are not against the law) for the processing of the personal data. The Act further establishes that once the reasons to process the personal data are no longer present, the personal data must be deleted.

TRANSFER

Personal data can only be transferred to a third party:

- For purposes directly related to the legitimate interests of the transferring party and the transferee, and
- With the prior consent of the data subject

However, such consent may be revoked. Additionally, the data subject must be informed of the purpose of the transfer, as well as of the identity of the recipient. The prior consent of the data subject is not necessarily required when the personal data to be transferred is limited to any of the following: name, surname, identity card number, nationality, address or date of birth.

The purpose and proper identification of the transferee must be included in the request for consent addressed to the data subject. Evidence of the data subject's consent must be kept in the files of the data processor.

If the data subject's consent is not obtained within ten business days (from the receipt of the communication from the data processor asking for consent), it will be construed that the data subject did not consent to the transfer of the data.

Upon the transfer, the data processor will remain jointly and severable liable for the compliance of the recipient's obligations under the Act.

The Act forbids the transfer of personal data to countries or international entities which do not provide adequate levels of protection (according to European standards). However, the Act allows international transfers to unsafe countries or entities when the data subject consents in writing to such transfer and when contractual clauses *(ie,* data transfer agreement) are in place that require an adequate level of data protection. The data transfer agreement must provide for the same levels of protection which are required under the laws of Uruguay.

In the case of an international transfer within a group of companies, Uruguayan laws establish that the international transfer is permitted without any authorization whenever the recipient branch has adopted a code of conduct that is duly registered with the local URCDP. The international transfer of personal data between headquarters and their respective branches or subsidiaries is authorized when the headquarters and their branches have a code of conduct (such as an intercompany agreement) duly filed with URCDP.

SECURITY

Data processors must implement appropriate technical and organizational measures to guarantee the security and confidentiality of the personal data, in accordance with the notion of proactive responsibility. These measures should be aimed at preventing the loss, falsification, and unauthorized treatment or access, as well as at detecting information that may have been lost, leaked, or accessed without authorization.

It is prohibited to register personal data in databases which do not meet technical safety conditions.

BREACH NOTIFICATION

If the data processor detects a breach of security measures, and if the consequences of the breach could substantially affect the rights of the data subject and/or the rights of any other agent or person involved, the data processor should report the breach to the affected persons and to the Data Protection Authority.

ENFORCEMENT

The URCDP is responsible for enforcement of the Act. In the context of its powers, the URCDP has broad investigatory powers, including audit and inspection, subpoena, search and seizure rights.

The URCDP has the authority to impose penalties against the data processor in the following order: warning, admonition, fines up to US$60,000, suspension of the database for five days, and closure of the database.

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as these activities typically involve the processing and use of personal data (*eg*, an email address is likely to be considered personal data for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing, but grants personal data owners / data subjects (individuals or legal entities) the right to demand the deletion or suppression of their data from the marketing database.

Personal data may be used and processed for marketing purposes when the personal data was either obtained from public documents provided by the data subject, or when prior consent has been obtained.

ONLINE PRIVACY

There are no provisions that specifically address online tracking or geolocation data. However, the general principles of the Act apply. The personal data processed cannot be used for purposes other than those that justified the acquisition of the data; when the reasons to process the personal data have expired, the personal data must be deleted.

KEY CONTACTS

Estudio Bergstein
www.bergsteinlaw.com/

Jonas Bergstein
Partner
Estudio Bergstein
T +598 2 901 2448
jbergstein@bergsteinlaw.com

Guzmán Ramírez
Estudio Bergstein
T +598 2901 2448
gramirez@bergsteinlaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UZBEKISTAN

Last modified 28 January 2019

LAW

Currently, Uzbekistan does not have a stand-alone data protection law.

Provisions regulating data protection issues are reflected in a number of legal acts, the most significant of which are the Constitution of the Republic of Uzbekistan entered into force on December 8, 1992, Law No. 439-II 'On Principles and Guarantees of Freedom of Information' dated December 12, 2002 (the 'Freedom of Information Law') and Law No. 560-II 'On Informatization' dated December 11, 2003.

Data protection provisions are partly captured by the Civil Code, the Labour Code, the Code on Administrative Liability, and the Criminal Code of the country, that establish liability for collection and dissemination of information about private life of individuals, disclosure of medical or commercial secrets, secrecy of correspondence, banking operations and savings, and etc.

There are also sector-specific laws applicable depending on the type of industry. Data protection regulation exists mainly in financial, telecommunication, health and insurance sectors and consists of the following legal acts:

- Law No. 530-II 'On Bank Secrecy' dated August 30, 2003, under which a bank is prohibited to disclose bank secrecy, and should guarantee its protection
- Law No. 822-I 'On Telecommunications' dated August 20, 1999, under which all operators and service providers are obliged to ensure the secrecy of communications
- Law No. 265-I 'On Protection of Citizens' Health' dated August 29, 1996, under which the medical secrecy is protected
- Law No. 358-II 'On Insurance Activities' dated April 5, 2002, under which insurance companies should guarantee the confidentiality of information which became available in course of provision of insurance services

On May 18, 2018, a draft law 'On Personal Data' (the 'Draft Law') was presented for general public discussion with the scheduled date for its adoption to be January 1, 2019. Based on the publicly available sources, on December 25, 2018 the Draft Law was reviewed by the Legislative Chamber of Oliy Majlis (Uzbekistan's Parliament). Yet, as of today the law has not been adopted.

Information presented herein is prepared based on the Draft Law, as currently available in public sources. All or some provisions of the Draft Law may be changed and redrafted prior to its adoption.

DEFINITIONS

Existing laws

The existing laws do not provide a precise definition of the term '**personal data**', yet classify personal data of individuals as confidential. As a matter of general practice, personal data is viewed as any information about facts, events and circumstances of an individual's life, allowing to identify the individual.

Laws related to formation and use of state information resources further provide a list of information that can be attributed to

personal data, as follows:

- Biographic data
- Identification data
- Personal characteristic
- Information about family status
- Social status
- Education background
- Skills
- Profession
- Occupation
- Financial standing
- Health condition, etc

The Draft Law

Unlike the existing laws, the Draft Law introduces a precise definition of the term '**personal data**'. As such, personal data is defined as the data related to or identifying an individual (towards whom processing of personal data is performed), which is recorded on an electronic, paper or other material.

The Draft Law further sets out an exhaustive list of information that can be qualified as personal data, as follows:

- Biographic data
- Biometric data
- Identification data
- Personal characteristic
- Information about family status
- Social status
- Occupation
- Financial standing
- Education background
- Profession
- Health condition
- Criminal record

Existing laws

The existing laws do not define the term '**sensitive personal data**'.

The Draft Law

The Draft Law defines '**sensitive personal data**' as data about:

- Racial or ethnical origin
- Political, religious or ideological convictions
- Membership in political parties and trade unions
- Physical or mental health
- Information regarding private life and criminal record

NATIONAL DATA PROTECTION AUTHORITY

Existing laws

Currently, there is no national data protection authority in Uzbekistan. However, there are sector-specific regulators that may regulate data protection issues in the relevant sectors. For example:

- The Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan – in the telecommunication sphere
- The Central Bank of the Republic of Uzbekistan – in the financial sphere
- The Ministry of Health of the Republic of Uzbekistan – in the health sphere, etc

The Draft Law

The Draft Law designates the Cabinet of Ministers of the Republic of Uzbekistan (the 'Cabinet of Ministers') and Authorized State Body as the main regulatory authorities in respect of the protection of personal data. It should be noted that the Authorized State Body is to be determined by the Cabinet of Ministers.

REGISTRATION

Existing laws

The existing laws do not require the registration of databases that contain personal data, except for state information systems providing public services in online mode. State information systems, which, among other things, process personal data, are subject to registration with the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan.

The Draft Law

The Draft Law requires a personal data database to be registered with the special State Registry of Personal Data Databases. The registration should represent a simple notification with a respective authority. The registration would not be required in cases, as follows:

- If related to employment
- When an agreement was entered into with the data subject
- When the data is publicly available
- When the data constitutes names and surnames of the individuals, etc

DATA PROTECTION OFFICERS

Existing laws

Under the existing laws, there is no requirement for organizations to appoint a data protection officer.

The Draft Law

According to the Draft Law, government bodies, local self-government bodies, organizations, legal persons should designate a structural unit or a responsible person that has to organize work with respect to personal data protection in the course of its processing.

COLLECTION & PROCESSING

Existing laws

Article 13 of the Freedom of Information Law establishes that collecting, storing and disseminating information on the private life of an individual is allowed only on the basis of consent of such individual, except as required by law. In practice, the term '**information on private life**' is equated with the term '**personal data**'.

Thus, in order for a data processor to collect, store and process any personal information on individuals, it must obtain a prior consent from a data subject (*ie,* the individual).

Existing legislation does not provide for specific requirements as regards the form of the consent. As a matter of practice, the consent is obtained in written form.

The Draft Law

Under the Draft Law, processing of personal data includes actions with respect to:

- Collection
- Systematization
- Accumulation
- Storage
- Clarification (update, alteration)
- Use
- Dissemination (including transfer)
- Depersonalization
- Blocking and deletion

Processing of personal data requires prior consent from an individual or his / her legal representatives. The consent should be made in writing or in the form of an electronic document. The amount of the personal data that can be included in the personal data database is to be determined in the consent.

Processing of personal data should pursue a certain purpose. This purpose should be fixed in the foundation documents or any other internal documents of a data controller and / or processor. Whenever the purpose of these operations changes, a new consent from individuals to conduct operations over the personal data related to them in line with such new purpose must be obtained.

A data processor may assign the processing of personal data to third parties only with the consent of individuals whose data is processed. Where assigned, a data processor is liable before the individuals for the actions of a person to whom the assignment is made.

The Draft Law determines that amendment and / or deletion of personal data requires the data processor to notify such individuals about this within three working days after these activities are executed.

The Draft Law requires a data processor to notify an individual on inclusion of his / her personal data into its personal data database, within ten working days from such inclusion. Such notification must be accompanied with information on the rights of the data subject, envisaged by the Draft Law, the purpose of operations over the personal data and third parties to which the personal data is transferred (if any). This requirement does not apply in cases where the personal data is collected from public sources. Transfer of personal data to third parties would require notification of the data subject, only if the initial consent of the data subject did not envisage such notification.

Lastly, collecting and processing of personal data for historical, statistical, sociological, or scientific research purposes requires the data processor to depersonalize such data, making it anonymous.

TRANSFER

Existing laws

Current laws do not prohibit the transfer of personal data outside of Uzbekistan. However, the procedure of such transfer is not defined by laws. The only requirement set by existing data protection regulations, is obtainment of consents of individuals whose personal data is transferred abroad.

The Draft Law

The Draft Law defines the cross-border transfer of personal data as the transfer of personal data to the territory of a foreign state authority, legal entity or individual of a foreign state. It allows the cross-border transfer of personal data on the condition that a foreign state can ensure the protection of personal data.

Nevertheless, cross-border transfer of personal data is still possible even in the absence of provision of foreign state protection.

For this purpose, there should be:

- The consent of a data owner on such cross-border transfer in place, or
- A sufficient cause, such as protection of the constitutional order, public order, rights and freedoms of citizens, health and morality of the population, or
- A ground envisaged in the international treaties of the Republic of Uzbekistan

The Draft Law also determines that cross-border transfer of personal data may be prohibited or restricted in order to protect the constitutional order of the Republic of Uzbekistan, morality, health, rights and legitimate interests of citizens, and to secure the defence of the country and national security.

SECURITY

Existing laws

The Freedom of Information Law contains a broad provision applicable with respect to security of different data. It states that any information, unlawful treatment of which can cause damage to its owner, user and other person, is subject to protection.

Further, it sets the purposes of such protection, which include:

- Prevention of threats to the security of individuals, society and the state in the sphere of information
- Preserving confidentiality of information, preventing its leak, theft, loss
- Preventing distortion and forgery of information

Security and protection of information are also envisaged in the laws related to formation and use of state information resources. Regulation 'On the Procedure for Documentation of Information, Tracking and Registration of State Information Resources' approved by the Resolution No.1558 of the Cabinet of Ministers of the Republic of Uzbekistan dated February 10, 2006 provides that protection of information resources, containing confidential information, should be provided through a set of organizational and technical measures aimed at solving the following main tasks:

- Prevention of leak, theft, loss, distortion, blocking, forgery of information resources and other unauthorized access to personal data
- Blocking of the channels of leakage of information
- Prevention of special software and technical impacts aimed at the destruction and distortion of information
- Identification of special devices for the removal or destruction of information embedded in technical facilities and allocated premises

The Draft Law

The Draft Law states that personal data is subject to the protection guaranteed by the state. It also imposes obligation on a data controller, processor and third party to take necessary legal, organizational and technical measures to ensure the protection of personal data. However, the Draft Law does not envisage the precise types and content of such measures, thus allowing a controller and a processor to determine them independently provided they are in line with data protection laws. In any case, processing and storage of information should be carried out exclusively by means that meet the requirements of information security.

BREACH NOTIFICATION

Both the existing laws and the Draft Law do not provide for the obligation to notify about a data breach.

ENFORCEMENT

Existing laws

Enforcement of existing laws related to personal data is ensured by a number of provisions contained in the Civil Code, the Criminal Code and the Code on Administrative Liability.

The Civil Code sets forth natural persons' non-property rights (such as right to privacy, person's life and health, honor and dignity etc) and provides for the remedies to protect them, which includes, inter alia, claiming damages, seeking injunctive relief and others.

According to Article 46 of the Code on Administrative Liability, disclosure of medical or commercial secrets, secrecy of correspondence and other communications, notarial actions, banking operations and savings, as well as other information that may cause moral or material damage to a citizen, his rights, freedoms and legitimate interests entails administrative liability in the form of a fine to be imposed on citizens (in the amount of up to 2 minimum monthly wages (approx US$49)), and on the companies' executive officers (in the amount of up to 5 minimum monthly wages (approx US$121)).

Also, collection and dissemination of information about the private life of individuals, constituting their private or family secret, without their consent is punishable by large fines amounting up to 40 minimum monthly wages (approx US$970). Repeated commission of the offense may lead to larger fines or imprisonment.

In the meantime, Article 141-1 of the Criminal Code prohibits violation of personal privacy by illegal collection and dissemination of personal information and family secrets. The liability for the above violation committed after imposition of an administrative penalty may be in the form of a fine (in the amount of up to 100 minimum monthly wages (approx. US$2426)), mandatory public works (up to 300 hours), or correctional labor (up to 2 years).

Pursuant to Article 179-3 of the Code on Administrative Liability, wrongful demanding, obtaining or disclosure of information constituting commercial, banking and other secrecy protected by law, in connection with combating money laundering and financing of terrorism, entails the imposition of a fine (in the amount of up to 15 minimum monthly wages (approx. US$363)).

The Draft Law

Under the Draft Law, a data subject is entitled to protect his / her personal data from:

- Illegal processing or accidental loss
- Destruction
- Damage
- Failure to provide
- Protection from the provision of information which is false or defamatory

In this regard, a data subject has a right to apply to a competent state bodies with such issues, resort to legal remedies, including claiming moral and material damages.

Under the Draft Law, the Authorized State Body is authorized to monitor compliance of others with the law and to examine complaints and applications of natural and legal persons regarding personal data processing issues. It also empowers the Authorized State Body to impose administrative and other liability on those violating the requirements of the Draft Law.

ELECTRONIC MARKETING

Existing laws

The Law No. ZRU-385 of the Republic of Uzbekistan 'On E-Commerce' (new version) dated May 22, 2015 contains a provision on the use of personal data in e-commerce and electronic marketing. It requires obtaining prior consent of a data subject for distribution of the offer and advertising, including through mass distribution of electronic messages.

The Draft Law

The Draft Law does not specifically regulate the use of personal data in electronic marketing. It is not in any way excluded from the scope of the Draft Law application. Therefore, the Draft Law is deemed to apply to the use of personal data in electronic marketing.

ONLINE PRIVACY

Both the existing laws and the Draft Law do not provide for regulation of online privacy. However, if personal data is involved and privacy issues are concerned, there are no obstacles for their application with respect to online privacy.

KEY CONTACTS

Dilshad Khabibullaev
Partner
Centil Law Firm
T +998711204778
dilshad.k@centil.law

Valeriya Ok
Senior Associate
Centil Law Firm
T +998711204778
valeriya.ok@centil.law

Sabina Saparova
Associate
Centil Law Firm
T +998711204778
sabina.saparova@centil.law

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ZAMBIA

Last modified 23 May 2019

LAW

Zambia regulates data privacy and protection issues under the Electronic Communications and Transactions Act (ECTA).

DEFINITIONS

Definition of Personal Data

The ECTA defines personal information as information about an identifiable individual, including, but not limited to:

- information relating to the race, gender, pregnancy, marital status, nationality, ethnic or social origin, color, age, physical or mental health, well-being, disability, religion, belief, culture, language and birth
- information relating to education, medical, financial transaction, criminal or employment history
- any identifying number, symbol, or other identifier assigned to the individual
- address, fingerprints or blood type
- personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award of a prize to be made to another individual
- correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature, or further correspondence that would reveal the contents of the original correspondence
- views or opinions of others about the individual
- views or opinions on grant proposals, awards, or prizes granted to another individual, provided such views or opinions are not associated with the other individual's name
- an individual's name, in combination with other personal data, or alone, if could reasonably be linked to personal data (exception applies for persons deceased for more than 20 years).

Definition of Sensitive Personal Data

The ECTA does not define sensitive personal information.

NATIONAL DATA PROTECTION AUTHORITY

The Zambia Information and Communication Technology Authority is responsible for enforcing the provisions of the ECTA.

REGISTRATION

There are no registration requirements in Zambia.

DATA PROTECTION OFFICERS

The ECTA does not require the appointment of a data protection officer.

COLLECTION & PROCESSING

Data controllers must adhere to the following principles in respect of collection and processing:

- obtain express written consent from the data subject to collect, collate, process or disclose any of the data subject's personal information, unless otherwise permitted or required by law
- only electronically request, collect, collate, process or store personal information on a data subject necessary for the lawful purpose for which the personal information is required
- disclose, in writing, to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored
- not use any personal information for any purpose other than the disclosed purpose, without express written permission from the data subject, unless permitted or required by law
- for as long as any personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected
- not disclose any personal information held by the data controller to a third party unless required or permitted by law or specifically authorized in writing by the data subject
- for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which, and the purpose for which, it was disclosed
- delete or destroy all personal information, except as otherwise provided under the ECTA or any other law, and
- may use any personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.

TRANSFER

All transfers must be based on the consent of the person whose data is to be transferred, unless otherwise required by law.

SECURITY

The ECTA provides for certain criteria for accreditation of authentication products and services.

BREACH NOTIFICATION

There is no breach notification requirement in Zambia.

ENFORCEMENT

General penalties under the ECTA include:

- in case of an individual, a penalty not to exceed five hundred thousand penalty units (approx. US$12,712) or to imprisonment for a period not to exceed five years, or both
- in case of a corporation or an unincorporated body, a penalty not to exceed one million penalty units (approx. US$25,424).

ELECTRONIC MARKETING

The ECTA includes provisions to regulate electronic transactions and requires that suppliers of goods provide certain information on their website.

The ECTA further includes provisions to protect customers in electronic transactions and requires inter alia that a description of the main characteristics of goods or services offered by a supplier be provided to the consumer to enable the consumer to make an informed decision on the proposed electronic transaction. This description must include the full price of the goods or services, including transport costs, taxes and any other applicable fees or costs.

ONLINE PRIVACY

Same principles as laid out above apply (see Electronic Marketing).

KEY CONTACTS

Louise Chilepa
Senior Associate
Chibesakunda & Co
T +260 211 366400
louise.chilepa@cco.co.zm

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ZIMBABWE

Last modified 28 January 2019

LAW

The protection of privacy is a principal enshrined in Zimbabwe's Constitution. While there is no designated national legislation dealing with data protection for private persons in Zimbabwe yet, there are existing laws that have a bearing on the right to privacy and protection of personal information for specified types of data, or in relation to specific activities.

The Access to Information and Protection of Privacy Act (Chapter 10:247) contains the most provisions on data protection. However, this generally only regulates the use of personal data by public bodies.

Other laws refer to the protection of information as a function of other activities or the protection of specific types of data, such as the Courts and Adjudicating Authorities (Publicity Restrictions) Act (Chapter 07:04), the Census and Statistics Act (Chapter 10:29), Banking Act (Chapter 24:20), National Registration Act (Chapter 10:17) and the Interception of Communications Act (Chapter 11:20).

In August 2016, Cabinet, which is the highest government approval body, approved the Revised National Policy for Information Communication Technology ("ICT Policy"). According to the approved ICT Policy, the establishment of an institutional framework for enacting legislation dealing specifically with digital data protection matters and cybersecurity is anticipated.

DEFINITIONS

Definition of personal data

The Access to Information and Protection of Privacy Act defines personal information as recorded information about an identifiable person which includes:

- The person's name, address or telephone number
- The person's race, national or ethnic origin, religious or political beliefs or associations
- The person's age, sex, sexual orientation, marital status or family status
- An identifying number, symbol or other particulars assigned to that person
- Fingerprints, blood type or inheritable characteristics
- Information about a person's healthcare history, including a physical or mental disability
- Information about educational, financial, criminal or employment history
- A third party's opinions about the individual
- The individual's personal views or opinions (except if they are about someone else)
- Personal correspondence with home or family

Definition of sensitive personal data

There is no law that defines sensitive personal data.

NATIONAL DATA PROTECTION AUTHORITY

There is currently no data protection authority, however, a provision in the Draft Data Protection Bill ("Draft Bill") that has been placed on the Government's Legislative Agenda for 2018-2019, creates a Data Protection Authority. According to the Draft Bill, this Authority will promote and enforce the fair processing of personal data and advise the Minister of Information Communication Technology on matters relating to privacy rights. The Authority will also conduct inquiries and investigations either on its own accord or on the request of any interested person in relation to data protection rights.

Under the Draft Bill, a data protection officer must be appointed to ensure the compliance with all obligations provided for in the Draft Bill. The Draft Bill further provides for the definition of sensitive data, which includes political opinions, religious beliefs and affiliations, and any information which may present a major risk to the risks of the data subject.

The Zimbabwe Media Commission's mandate does the following:

- Ensures that the people of Zimbabwe have equitable and wide access to information
- Comments on the implications of proposed legislation or programs of public bodies on access to information and protection of privacy
- Comments on the implications of automated systems for collection, storage, analysis or transfer of information or for the access to information or protection of privacy

The Revised ICT Policy proposes the establishment of a quasi-government entity to monitor Internet traffic. It states that all Internet gateways and infrastructure will be controlled by a single company, while a National Data Centre to support both public and high security services and information will be established.

REGISTRATION

There is no law that requires the registration of databases.

DATA PROTECTION OFFICERS

There is no provision to appoint data protection officers.

COLLECTION & PROCESSING

There are no specific provisions for the collectors of personal data to obtain the prior approval of data subjects for the processing of their personal data.

The Census and Statistics Act contains provisions which restrict the use and disclosure of information obtained during the conducting of a census exercise. Under this Act, authorities are able to collect, compile, analyze and abstract statistical information relating to any of the following:

- Commercial
- Industrial
- Agricultural
- Mining
- Social
- Economic
- General activities and conditions of the inhabitants of Zimbabwe and to publish such statistical information

TRANSFER

The transfer of personal data to any other jurisdiction is not specifically restricted.

SECURITY

The Revised ICT Policy states that there will be development, implementation and promotion of appropriate security and legal systems for e-commerce, including issues related to cybersecurity, data protection and e-transactions. The Policy states that the following laws will be enacted to cater for intellectual property rights, data protection and security, freedom of access to information, computer related and cybercrime laws: (i) data protection and privacy, (ii) intellectual property protection and copyright, (iii) consumer protection and (iv) child online protection.

BREACH NOTIFICATION

Breach notification

There is no law which requires data protection officers to report a breach.

Mandatory breach notification

There are no mandatory breach notification provisions.

ENFORCEMENT

The Constitution mandates the Human Rights Commission (HRC) to enforce a citizen's human rights where they have been violated. The right to privacy, including the right not to have the privacy of one's communication infringed, is a basic human right and, thus, falls within the purview of the HRC. However, the Monitoring of Interception of Communications Centre (MICC), established by the Interception of Communications Act, is mandated to, among other things, monitor communications made over telecommunications, radio communications and postal systems and to give technical advice to service providers. The mandate of the MICC does not preclude it from monitoring computer-based data for the purposes of enforcing an individual's right to privacy where it is found that such right has been infringed.

ELECTRONIC MARKETING

The government is currently working on a Consumer Protection Act, intended to introduce requirements to protect consumers from unfair trade practices. The draft Consumer Protection Act does not make reference to electronic marketing, nor does it provide for consumer privacy rights with respect to personal data.

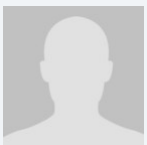
ONLINE PRIVACY

There is currently no specific online privacy legislation.

KEY CONTACTS

Manokore Attorneys
www.manokore.com

Farai Nyabereka
Partner
Manokore Attorneys
T T +263 4 746 787
fnyabereka@manokore.com



Lloyd Manokore
Partner
Manokore Attorneys
T +263 4 746 787
lmanokore@manokore.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.