COMPARISON:

# Indian Personal Data Protection Bill 2019 vs. GDPR

By Kurt Wimmer, CIPP/E, CIPP/US, Gabe Maldoff and Diana Lee
Covington & Burling

*This chart provides a high-level comparison between the EU General Data Protection Regulation and India's Personal Data Protection Bill.*

| LEGEND | Degree of operational change from the GDPR | | | |
|---|---|---|---|---|
| | Little or no operational change likely required. | Minor operational adjustments likely required. | Significant operational adjustments likely required. | Major operational change likely required. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| Scope and application | | | |
| TERRITORIAL SCOPE | The GDPR applies to:<br>• Organizations that have an establishment in the European Union and process personal data "in the context of" the EU establishment.<br>• Organizations that are not established in the EU but process personal data in relation to either (a) offering goods or services in the EU; or (b) monitoring the behavior of individuals in the EU. | The PDPB applies to:<br>• Processing personal data that has been collected, disclosed, shared or otherwise processed within the territory of India[1] (S. 2(A)(a)).<br>• Indian companies, Indian citizens, and any other persons or bodies incorporated or created under Indian law (S. 2(A)(b)). | • The PDPB's scope of application is potentially broader than that of the GDPR, as an entity may fall within scope merely by processing personal data in India (e.g., even through the use of a processor in India).<br>• However, this broad scope of application may be narrowed should the government exercise its authority to exempt such processing activities. |

[1] Although it is not clear whether an organization must be based in India for this jurisdictional basis to apply, the reference to "data fiduciaries or data processors not present within the territory of India" in Section 2(A)(c) suggests that this basis for jurisdiction should be read more narrowly to apply only to organizations with a presence in India.

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| | | • Organizations that are not present in India, but process personal data in connection with (i) business carried out in India or any systematic offering of goods or services to individuals in India; or (ii) an activity that involves profiling individuals in India (S. 2(A)(c)).<br><br>**NOTE:** The Central Government is permitted to exempt any data processor or class thereof from the scope of the PDPB in the context of outsourced services, where (a) the processor(s) is contracted by a person or entity outside of India; and (b) the processing relates only to individuals outside of India (S. 37). | |
| SUBJECT-MATTER SCOPE | Applies to:<br>• Personal data — anonymous data is out of scope.<br>• Automated processing or non-automated processing where personal data forms part of a filing system.<br><br>Does not apply to:<br>• Personal data processed by natural persons for purely personal or household purposes.<br>• Processing by law enforcement and national security agencies. | Applies to:<br>• Personal data — anonymous data is generally out of scope, except that the Central Government may direct organizations to disclose "anonymized" personal data or "non-personal data."<br><br>Does not apply to:<br>• Personal data processed by natural persons for purely personal or domestic purposes, or for journalistic purposes (pursuant to a code of ethics) — except that data security requirements continue to apply.<br>• Processing by law enforcement and national security agencies, as well as by courts or tribunals (to the extent necessary to exercise a judicial function).<br>• Processing in the interests of prevention, detection, investigation and prosecution of any offense or any other contravention of law. | • The PDPB grants the government broad authority to compel the disclosure of information that does not constitute personal data.<br>• Exemptions for the prevention/detection of criminal activity are not limited to law enforcement agencies and could apply to any organization engaged in such processing. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| DEFINITION OF PERSONAL DATA | • Personal data is 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, taking into account "all of the means reasonably likely to be used."[2] | • Personal data is data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling. | The definition of personal data under the PDPB is broader than the corresponding GDPR definition:<br>• The GDPR concept of personal data takes into account the reasonable likelihood that an individual will be identifiable. This flexibility does not appear in the PDPB.<br>• Inferences are expressly within scope of the definition of personal data under the PDPB, where they are derived from personal data for profiling purposes. Under the GDPR, inferences may be personal data to the extent they relate to an identifiable individual, but not all inferences derived from personal data will also be personal data.<br>• The PDPB grants the DPA wide latitude to define a process of anonymization that would take data outside the scope of the PDPB, which could either narrow or broaden the scope of the definition of personal data. |

[2] *See* GDPR, Recital 26.

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| DEFINITION OF SENSITIVE PERSONAL DATA | "Special categories of personal data" is defined as personal data revealing:<br>• Racial or ethnic origin.<br>• Political opinions, religious or philosophical beliefs.<br>• Trade union membership.<br>• Genetic data.<br>• Biometric data (for the purpose of uniquely identifying a natural person).<br>• Health.<br>• Sex life or sexual orientation.<br><br>Personal data relating to criminal convictions and offenses, while not special category data, is subject to distinct rules defined by EU or member state law. | "Sensitive personal data" is defined as personal data which may reveal, be related to, or constitute:<br>• Financial data.<br>• Health data.<br>• Official identifier.<br>• Sex life.<br>• Sexual orientation.<br>• Biometric data, which as defined, includes the concept of being used to uniquely identify an individual.<br>• Genetic data.<br>• Transgender or intersex status.<br>• Caste or tribe.<br>• Religious or political belief or affiliation.<br><br>The PDPB permits the government in consultation with the data protection authority to define additional categories of sensitive personal data, taking into account:<br>• The risk of significant harm that could result from processing such data, including harms to a discernible class.<br>• Any expectations of confidentiality attached to the data.<br>• The adequacy of protections afforded by the provisions applicable to ordinary personal data. | In general, there is significant overlap between the way sensitive data is defined under each framework, but the definition of sensitive data is broader under the PDPB:<br>• The PDPB includes "financial data" within the scope of sensitive data.<br>• The PDPB allows the government to define additional categories of sensitive data, whereas the list of categories under the GDPR is finite.<br><br>One exception is that the GDPR provides for additional rules for processing criminal convictions and offenses data, but the PDPB includes no similar provision. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| RELEVANT PARTIES | • Controller: The natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.<br>• Processor: A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.<br>• Data subject: An identified or identifiable natural person. | • Data fiduciary: Any person, including the state, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.<br>• Data processor: Any person, including the state, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary.<br>• Data principal: The natural person to whom the personal data relates. | • The definitions of the relevant parties generally align, despite the use of different terms for functionally similar concepts.<br>• Although use of the term "fiduciary" may imply the existence of a duty of care and/or loyalty, no such duty is expressly provided except within the provisions relating to children's data. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| | Lawfulness of processing | | |
| GENERAL PRINCIPLES | The GDPR sets out seven principles in Article 5:<br>• Lawfulness, fairness and transparency.<br>• Purpose limitation.<br>• Data minimization.<br>• Accuracy.<br>• Storage limitation.<br>• Integrity and confidentiality.<br>• Accountability. | The PDPB does not refer to "principles," but a number of provisions impose similar requirements:<br>• Personal data may not be processed by any person "except for any specific, clear and lawful purpose" (S. 4).<br>• Personal data must be processed "in a fair and reasonable manner and ensure the privacy of the data principal" (S. 5(a)).<br>• Personal data must be processed "for the purpose consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected" (S. 5(b)).<br>• Personal data must be "collected only to the extent that is necessary for the purposes of processing of such personal data" (S. 6).<br>• Data fiduciaries must "take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed," taking into account whether (a) the data is likely to be used to make a decision about the data principal; (b) the data is likely to be disclosed; or (c) is kept in a form that distinguishes facts from opinions or personal assessments (S. 8). | • At a high level, there is a significant degree of conversion between the two frameworks.<br>• With respect to lawfulness of processing, as discussed below, the PDPB places greater emphasis on the role of consent; however, consent under the PDPB is more closely linked to transparency than GDPR's concept of consent, which emphasizes specific and meaningful control.<br>• The PDPB's accuracy requirements are more specific than those under the GDPR — in particular, these require accuracy to be assessed in relation to a number of factors, including whether the data is a fact or an opinion or assessment.<br>• The PDPB's storage limitation provisions are also more specific than those under GDPR:<br>1. Unlike GDPR, which permits retaining the data in a form that no longer identifies an individual, the PDPB requires deletion.<br>2. The PDPB also requires data fiduciaries conduct periodic reviews of whether personal data must be retained.<br>• The PDPB does not have a provision analogous to the GDPR's integrity and confidentiality principle, but there are specific provisions governing information security, which are addressed in detail below. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| | | • Data fiduciaries may "not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing" in the manner specified by regulations, unless the data principal provides explicit consent or the processing is required by law (S. 9). Data fiduciaries must "undertake periodic review to determine whether it is necessary to retain the personal data in its possession."<br>• Data fiduciaries are "responsible for complying with the provisions of this Act in respect of any processing undertaken by it or on its behalf" (S. 10). | |
| LEGAL BASIS FOR PROCESSING OF PERSONAL DATA | There are six lawful bases for processing personal data, subject to member states adding more:<br>• Consent.<br>• Performance of a contract.<br>• Legal obligation.<br>• Legitimate interests.<br>• Life protection and vital interests.<br>• Public interest. | There are seven lawful bases for processing personal data:<br>• Consent.<br>• Legal obligation.<br>• Medical emergency involving a threat to life or severe threat to health.<br>• Providing medical treatment or health services.<br>• Protecting the safety of individuals during a disaster.<br>• Employment purposes.<br>• "Reasonable purposes" as may be specified by regulations, including for preventing or detecting unlawful activity, whistleblowing, mergers and acquisitions, network and information security, credit scoring, recovery of debt, the operation of search engines, or processing of publicly available personal data. | • The PDPB does not provide for a basis for processing that is necessary for the performance of a contract (although consent is defined less restrictively and may permit processing that is necessary to enter into or perform contracts).<br>• The "reasonable purposes" basis under the PDPB is similar to the GDPR's legitimate interest basis, but is limited to purposes that are specified by regulation.<br>• Additional bases for health and safety and for employment purposes under the PDPB may have been justified under the GDPR's broader legitimate interests or public interests bases, which do not appear under the PDPB. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| CONSENT | The GDPR imposes a number of requirements for obtaining valid consent:<br>• Consent must be freely given, specific and informed.<br>• It must be granted by an unambiguous affirmative action.<br>• Generally, provision of a service cannot be made conditional on obtaining consent for processing that is not necessary for the service.<br>• A request for consent must be distinct from any other terms and conditions.<br>• Consent for separate processing purposes must be provided separately.<br>• Individuals have the right to withdraw consent at any time "without detriment" and it should be as easy to withdraw consent as it was to give it. | Under the PDPB, valid consent must be:<br>• Free, taking into account whether it complies with Indian contract law requirements (i.e., freedom from coercion, undue influence, fraud, misrepresentation or mistake).<br>• Informed in accordance with the provisions on transparency.<br>• Specific.<br>• Clear, taking into account whether it is indicated by a meaningful affirmative action under the circumstances.<br>• Capable of being withdrawn, taking into account the comparative ease of withdrawing and providing consent. | The PDPB definition of consent is considerably more flexible than that under the GDPR and incorporates elements of the GDPR's "contractual necessity" basis:<br>• The standard for freely given matches a contractual standard under the PDPB, rather than the GDPR's more stringent "without detriment" standard.<br>• There's an argument that consent would be considered "informed" as long as a privacy notice is made available and that it is not necessary in all cases to provide the request for consent separately from the privacy notice or other terms.<br>• "Specificity" is defined by reference to what the data subject would expect.<br>• There does not seem to be a concrete requirement to ask consent for separate purposes separately.<br>• A data fiduciary may be permitted to penalize the data principal for withdrawing consent without a "valid reason" (S. 11(6)).<br>• S. 11(4) suggests that provision of a service can be made conditional on consent where the processing is "necessary for that purpose." |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| LEGITIMATE INTERESTS | • Processing is permitted, without consent, where it is necessary for the controller's (or a third party's) legitimate interests and provided such interests are not overridden by the rights and interests of the data subject.<br>• It is the controller's responsibility to determine whether the interests it pursues under this basis are legitimate and proportionate, and controllers are expected to document their assessments. | The PDPB permits the DPA to specify "reasonable purposes" for processing.<br><br>In defining these reasonable purposes, the DPA must take into consideration:<br>• The interests of the data fiduciary or any public interests.<br>• Whether the data fiduciary can reasonably be expected to obtain consent for the processing.<br>• The effect of the processing on the rights of data principals.<br>• The data principal's reasonable expectations under the context.<br><br>Reasonable purposes may include certain specified activities, such as fraud prevention, information security, M&A, recovering debt and processing publicly available personal data, among others, and the DPA may enumerate others not provided in the bill. | • The PDPB is significantly more stringent than the GDPR in that it assigns responsibility for defining reasonable purposes to the DPA rather than to the controller/data fiduciary.<br>• The factors the DPA must consider under the PDPB are generally similar to those enumerated under guidance by EU regulators, but there is no requirement for the DPA to enumerate any or all of the reasonable purposes set out in the bill.<br>• Organizations tend to rely on legitimate interests under GDPR for a wide range of activities that are not enumerated in the PDPB, including marketing and product development and improvement.<br>• The fact that the DPA must consider whether the data fiduciary can be expected to obtain consent for the processing — a factor that does not form part of the GDPR analysis — could further restrict the types of activities that are authorized under this provision. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| CONDITIONS FOR PROCESSING SENSITIVE DATA | There are 10 lawful bases for processing sensitive data, subject to member states adding more:<br>• Explicit consent.<br>• Comply with obligations and exercising rights in the employment and social security context.<br>• Life protection and vital interests.<br>• Legitimate activities (by a foundation, association or other not-for-profit body with a political, philosophical, religious, or trade union aim, processing data about its members).<br>• Establishment, exercise or defense in legal claims.<br>• Manifestly made public by the individual.<br>• Substantial public interest defined by law.<br>• Preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment.<br>• Substantial public interest in health.<br>• Archiving, scientific or historical research purposes. | The grounds for processing sensitive personal data are the same as those required for non-sensitive personal data, except:<br>• Where consent is required, it must be obtained explicitly:<br>  • In clear terms, and not inferred from conduct.<br>  • Separately from other processing.<br>  • After informing the data principal of the purpose for processing that is likely to cause significant harm.<br>• Sensitive personal data may not be processed for the employment purposes legal basis. | • The standards for explicit consent to process sensitive data are closely aligned.<br>• In the absence of an employment purposes basis for processing sensitive data under the PDPB, employers will likely rely more heavily on explicit consent for employee benefits programs.<br>• No ground equivalent to the GDPR's "manifestly made public" condition exists in the PDPB, but the DPA could specify such a ground as a "reasonable purpose."<br>• The PDPB permits the DPA to exempt classes of research from the application of the bill, but unless and until the DPA takes such action, there is no basis for processing for research purposes.<br>• The wider definition of sensitive personal data under the PDPB means that a broader spectrum of activities will be affected by these conditions for processing. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| | Protections for children | | |
| CHILDREN | • The GDPR imposes additional obligations when collecting consent from children under the age of 16 or at an age set between 13 and 16 by member state law.<br>• Where providing certain electronic services at a distance (i.e., "information society services") directly to a child and where the processing is based on consent, consent must be provided by a parent or guardian.<br>• Processing personal data of children is pertinent to other GDPR requirements (e.g., notices must be tailored to children; the fact that data subjects are children could tip the balance of the legitimate interests test or trigger a data protection impact assessment).<br>• One recital states significant automated decisions should not be taken concerning children. | • A child is defined as someone under the age of 18.<br>• There is a general obligation to process personal data "in such a manner that protects the rights of, and is in the best interests of" children.<br>• Data fiduciaries are required to verify a child's age and obtain the consent of a parent or guardian before processing any personal data of a child. The DPA is empowered to promulgate regulations that specify how this is to be done.<br>• Data fiduciaries that operate online services directed at children or process large volumes of children's data may be classified as "guardian data fiduciaries" by regulations — guardian data fiduciaries are barred from profiling, tracking or targeting advertising at children. | • The PDPB sets the age threshold for being considered a child higher than the GDPR permits.<br>• The PDPB's requirement to verify a child's age before any processing imposes a significant new requirement not present in the GDPR.<br>• Unlike the GDPR, the PDPB's requirement to obtain parental consent applies to all processing of children's data, not just where consent is the legal basis.<br>• The ban on profiling of children for guardian data fiduciaries is broader than any similar restrictions under the GDPR as it is not limited to significant automated decisions. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| | Individual rights | | |
| TRANSPARENCY REQUIREMENTS | • Information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.<br>• Where personal data is collected directly from the individual, notice must be provided at of before the time of collection.<br>• For personal data collected indirectly (i.e., from another source), notice must be provided within one month (or upon first contact with the individual, if earlier), unless providing notice would be impossible or would require disproportionate effort.<br>• Detailed requirements for the content that must be included in notices. | • Notices must be clear, concise and easily comprehensible to a reasonable person.<br>• There is a requirement to translate notices to multiple languages where necessary and practicable.<br>• Notice must be provided at the time of collection, or, if not collected directly from the individual, as soon as reasonably practicable, unless providing notice would "substantially prejudice the purpose of processing" (S. 7(3)).<br>• Detailed requirements for the contents of notices, including:<br>  • Detailed disclosures of the "individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared" (S. 7(1)(g)).<br>  • The procedure for redressing grievances (in addition to responding to rights requests) (S. 7(1)(k)).<br>  • Any rating of a data trust score that may be assigned to the data fiduciary (S. 7(1)(m)).<br>  • Any other information that may be specified by regulations (S. 7(1)(n)). | • There is significant overlap between the transparency requirements of both frameworks.<br>• However, the PDPB does include additional disclosure requirements that may not already be included in a privacy notice drafted for GDPR, such as details on the procedure for handling individual requests and grievances, and, if applicable, a data trust score assigned by a data auditor pursuant to the PDPB's audit provisions (discussed below).<br>• In addition, requirements to provide the contact details of the data protection officer, and to provide notice in multiple languages, may require the localization of global privacy notices.<br>• Finally, the requirements for disclosing recipients under the PDPB may require more specific disclosures of data processors than is required under the GDPR. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| RIGHT OF ACCESS | • Individuals have the right to receive information about how their personal data is processed and a copy of their personal data.<br>• Personal data must be provided:<br>  • Free of charge, except where requests are manifestly unfounded or excessive or for additional copies.<br>  • In electronic form when so requested.<br>  • Within one month unless an extension applies.<br>• Exceptions apply where providing the information above would adversely affect the rights and freedoms of others, including intellectual property rights. | • Individuals have the right to receive:<br>  • Confirmation of whether their personal data is being processed and a summary of the processing activities that were undertaken.<br>  • Copies of the personal data processed by the data fiduciary "or any summary thereof" (S. 17(1)(b)).<br>• The information provided above must be provided free of charge.<br>• The data fiduciary must also "in one place the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary together with the categories of personal data shared with them" (S. 17(3)).<br>• The time period for responding will be specified by regulations.<br>• There is an exception where compliance would "harm the rights of any other data principal" (S. 21(5)). | • The rights of access are broadly similar.<br>• However, the requirement to provide the identities of all data fiduciaries with whom personal data has been shared could result in significant new administrative burdens. It is not clear whether the "by any data fiduciary" language would also require documenting any onward transfers by data fiduciaries to whom personal data is disclosed.<br>• Although the PDPB does not include format requirements, these appear in the more broadly formulated portability right under the PDPB.<br>• The PDPB exception for protecting other data principals may not permit withholding personal data on intellectual property grounds. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| RIGHT OF PORTABILITY | • The right to portability applies only to:<br>  • Processing based on consent or a performance of a contract.<br>  • Where the data is provided to the controller by the data subject, which includes information observed about the data subject, but not inferences.<br>  • The processing is carried out by automated means.<br>• Where the right applies, personal data must be provided in a structured, commonly used and machine-readable format, with the right to transmit such data to others without hindrance.<br>• Where technically feasible, an individual may ask for the data to be transmitted directly to another controller.<br>• As with the right of access, there is an exception to protect the rights and freedoms of third parties. | • The right to portability applies to personal data processed through automated means, where:<br>  • The personal data was provided to the data fiduciary.<br>  • The "data" has been generated in the course of provision of services or use of goods.<br>  • The "data" forms part of any profile on the data principal or which the data fiduciary has otherwise obtained.<br>• Where the right applies, personal data must be provided in a structured, commonly used and machine-readable format and may be transferred directly to another data fiduciary.<br>• Exceptions are provided where compliance would reveal a trade secret or would not be technically feasible. | • The right to portability under the PDPB is broader than the corresponding GDPR right as it is not limited to data that is processed under certain legal bases.<br>• The PDPB portability right also applies to profile information, even if the data may be inferred. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| RIGHT OF CORRECTION | • Grants data subjects the right to:<br>  • Correct inaccurate personal data.<br>  • Complete incomplete personal data.<br>• Where personal data is updated, it must be communicated to each recipient to which it was disclosed, unless this would involve disproportionate effort.<br>• The controller must restrict processing where the accuracy of the data is disputed for the time needed to verify the request. | • Grants data principals the right to:<br>  • Correct inaccurate or misleading personal data.<br>  • Complete incomplete personal data.<br>  • Update out-of-date personal data.<br>• The data fiduciary must take steps to communicate the updated data to relevant entities or individuals to whom the personal data was disclosed, particularly where there may be impacts for the rights and interests of the individual.<br>• Where the data principal disputes the accuracy of the data and the data fiduciary does not take action, the data fiduciary must take reasonable steps to indicate that the accuracy of such personal data is disputed. | • These rights are broadly aligned with only cosmetic differences. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| RIGHT TO BE FORGOTTEN | • The GDPR grants data subjects the right to request the deletion of personal data processed by the controller, where the data is no longer needed for the purpose for which it is processed, where the data subject withdraws consent or objects, and where processing is unlawful or deletion is required by law.<br>• If the controller grants a request for the deletion of data that was previously made public, the controller would need to "take reasonable steps" to inform any third parties that may be processing the data of the data subject's request. There is also an obligation to communicate the request directly to any known recipients of the data, unless it would be impossible or would require disproportionate effort.<br>• Controllers may rely on a number of exceptions, including establishing, exercising or defending legal claims, conducting research meeting certain conditions, and other compelling legitimate interests to override a request. | • The right to erasure (S. 18(d)) grants a right to request the deletion of personal data that is no longer necessary for the purpose for which it was processed.<br>  • If the data fiduciary fulfils the request, it must notify all relevant entities or individuals to whom the personal data was disclosed, particularly where this will impact the rights and interests of the individual.<br>• The right to be forgotten (S. 20) grants individuals a right to restrict or prevent the continued disclosure of personal data (i.e., this is not a deletion right).<br>  • The right applies where data is no longer needed for the purposes for which it was processed, the data principal withdraws consent where processing was based on consent or the disclosure was unlawful.<br>  • To enforce the right, individuals must apply to an adjudicating officer appointed by the DPA.<br>  • The adjudicating officer must take into account a number of contextual factors in weighing whether restriction is justified.<br>  • In particular, the right to be forgotten must be balanced against freedom of expression concerns. | • The PDPB distinguishes between two separate rights — one for erasure and one for restricting the disclosure of personal data (i.e., the right to be forgotten).<br>• Unlike the GDPR, the PDPB places responsibility for determining the scope of application of the right to be forgotten on adjudicating officers appointed by the DPA, rather than the controller.<br>• By requiring adjudicating officers to consider a number of contextual factors and to balance various interests, it is likely that the PDPB right to be forgotten will be interpreted more narrowly than the corresponding GDPR right. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| RIGHTS RELATING TO PROFILING | • Data subjects have a right not to be subject to solely automated decisions, including profiling, that produce legal or significant effects, unless certain conditions are met.<br>• Where such decisions are permitted, data subjects have a right to obtain human intervention and contest the decision.<br>• Controllers must also provide meaningful information about the logic of decisions and take reasonable steps to prevent bias, error or discrimination. | • There is no overarching right not to be subject to profiling or significant decisions, except in the case of children. | • The PDPB does not provide a right to prevent automated decisions similar to the one found in the GDPR.<br>• However, as discussed above, guardian data fiduciaries may not profile children. |
| Accountability requirements | | | |
| APPOINTMENT OF A REPRESENTATIVE | • Controllers and processors not established in the EU that are subject to the GDPR must appoint a representative in the EU, except if processing is occasional and does not involve large scale processing of sensitive data. | • N/A. | • The PDPB does not include a requirement to designate a representative. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| DPA REGISTRATION | • N/A. | • "Significant data fiduciaries" are required to register with the DPA in accordance with procedures that will be set out in regulations (S. 26(2)).<br>• The DPA is required to notify data fiduciaries or classes of data fiduciaries as significant taking into account the following factors:<br>  • The volume and sensitivity of data processed.<br>  • Company revenue.<br>  • Risk of harm.<br>  • Use of new technologies. | • The PDPB introduces a requirement for a class of entities (significant data fiduciaries) to register with the DPA. |
| APPOINTMENT OF A DPO | • Required for private entities only where a "core activity" of the controller or processor involves either (a) the regular and systematic monitoring of data subjects on a large scale; or (b) the large-scale processing of sensitive data.<br>• The DPO must have sufficient independence and skill to carry out its functions and must be able to report to the highest levels of management within the organization.<br>• DPOs may be outsourced.<br>• Guidance from EU regulators recommends that the DPO should be based in the EU. | • Appointment of a DPO is required for all significant data fiduciaries.<br>• There are no express independence or skill requirements, but further guidance may be provided by regulations.<br>• The DPO must be based in India.<br>• The DPO must "represent the data fiduciary under this Act." | • The PDPB leaves it to the DPA to determine the thresholds for being considered a "significant data fiduciary" — it is difficult at this stage how this will compare to the GDPR's thresholds for appointing a DPO.<br>• The requirement to appoint a DPO may pose a challenge for global organizations.<br>• The requirement to "represent" the data fiduciary raises questions about whether the Indian DPO could be subject to personal liability. |
| RECORD OF PROCESSING | • Controllers and processors must retain detailed records of their processing activities unless very narrow exceptions apply. | • Only significant data fiduciaries are required to retain specific records of processing (S. 28(1)).<br>• The requirement to retain records of processing applies to "important operations," periodic review of security safeguards and DPIAs, and other records that may be specified by regulations. | • The PDPB record of processing requirements appear to be more flexible than those under the GDPR and will likely apply to a small proportion of companies subject to the framework. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| DATA PROTECTION IMPACT ASSESSMENT | • The GDPR requires controllers to conduct a DPIA for certain "high risk" activities, including (a) systematic and extensive profiling; (b) processing sensitive data on a large scale; and (c) systematic monitoring of a publicly accessible area on a large scale.<br>• In cases where the risks cannot be mitigated, the controller must consult with the DPA before engaging in the processing. | • Applies only to significant data fiduciaries, where processing involves (a) new technologies; (b) large-scale profiling or use of sensitive data; or (c) any other activities that carry a significant risk of harm as may be specified by regulations.<br>• All DPIAs must be submitted to the DPA for review, and the DPA may direct the data fiduciary to cease processing. | • Unlike under the GDPR, the PDPB requires all DPIAs to be submitted to the DPA for review. |
| PRIVACY BY DESIGN | • Requirement to implement appropriate compliance processes through the lifecycle of any product, service or activity.<br>• By default, only the personal data necessary for a purpose should be processed and personal data should not be publicly disclosed without an individual's affirmative action. | • Data fiduciaries must "prepare a privacy by design policy" containing certain defined elements (S. 22(1)).<br>• Data fiduciaries may also elect to seek certification from the DPA for the privacy-by-design policies, in which case the policy would be published on both the data fiduciary's and the DPA's website (S. 21(2)-(4)).<br>• The incentive for seeking certification is that this would permit a data fiduciary to participate in the regulatory sandbox, which provides some shelter from enforcement around the use of new technologies (S. 40). | • The PDPB's privacy-by-design requirements appear to be aimed in particular at the development of policies and documentation, whereas the GDPR accords controllers with greater flexibility in how they will implement the requirement. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| AUDIT REQUIREMENTS | • None that is applicable to controllers.<br>• Processors must agree to audit provisions in contracts with controllers. | • Significant data fiduciaries must submit their processing to annual audit by independent auditors selected from a list approved by the DPA.<br>• Data auditors may assign a "data trust score" to a data fiduciary based on their findings.<br>• The DPA may also direct data fiduciaries that are not "significant" to conduct an audit if the DPA considers the data fiduciary's processing to be likely to cause harm. | • The GDPR contains no similar audit requirement. |
| APPOINTMENT OF PROCESSORS | • Processing by processors must be subject to detailed contracts, with requirements set out in Article 28 of the GDPR. | • Contracts with processors only need to specify that (a) the processor will process personal data in accordance with the data fiduciary's instructions; (b) personal data must be held in confidence; and (c) sub-processors cannot be appointed without approval. | • Although the PDPB includes requirements for contracting with processors, these requirements are less prescriptive than the equivalent GDPR provisions. |
| Security and breach notification | | | |
| INFORMATION SECURITY | • Controllers are processors are required to implement appropriate technical and organizational measures to protect the security of personal data. | • Data fiduciaries and data processors are required to implement necessary security safeguards. | • There is little functional difference between the provisions. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| BREACH NOTIFICATION | • Controllers must notify the DPA of a breach within 72 hours, unless the breach is unlikely to result in a risk to individuals.<br>  • Notification may be made in stages as information becomes available.<br>• Controllers must notify individuals of a breach without undue delay only if it is likely to result in a "high risk" to individuals.<br>• Processors must notify a controller of a breach without undue delay. | • Data fiduciaries must notify the DPA of a breach "as soon as possible" if it is "likely to cause harm to any data principal."<br>  • The time period for notifying breaches may be established by regulations.<br>  • The time period for notification should also take into account any period that may be required to adopt urgent measures to remedy or mitigate the breach.<br>  • Notification may be made in stages.<br>• The DPA may direct the data fiduciary to post about the breach on its website (or may post on its own website). | • The PDPB leaves it to the DPA to establish the deadline for notification of breaches.<br>• The threshold for a reportable breach is higher under the PDPB, as it must be "likely" that the breach will cause harm to individuals.<br>• It is the DPA's responsibility to decide whether individuals should be notified of a breach, though data fiduciaries appear to be permitted to proactively notify, such as to help mitigate risks.<br>• There is no express requirement on processors to notify data fiduciaries of a breach but it may be implicit from the data fiduciary's responsibility for processing that it will need to secure this commitment from its processors by contract. |
| International data transfers | | | |
| DATA LOCALIZATION REQUIREMENTS | • Localization is not required unless international data transfer requirements are not met. | • "Critical personal data" must be processed in India, except under emergency circumstances or where the government has approved the transfer, taking into account India's security and strategic interests.<br>  • The government is granted broad discretion to define "critical personal data," but the concept appears to be related to national security.<br>• Sensitive personal data must be stored in India, but a copy of such data may be transferred outside of India in accordance with the data transfer requirements below. | • Localization requirements represent a significant area of divergence between the PDPB and GDPR. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| INTERNATIONAL DATA TRANSFER | The transfer of personal data outside the European Economic Area is permitted only where:<br>• The recipient is in a territory considered by the European Commission to offer an adequate level of protection for personal data (after an assessment of its privacy laws and law enforcement access regime).<br>• Appropriate safeguards are put in place, such as European Commission-approved standard contractual clauses or binding corporate rules approved by DPAs.<br>• A derogation applies, such as where data subjects provide explicit consent, the transfer is necessary to fulfil a contract (and occasional), or there is a public interest founded in EU or member state law, among others. | A copy of sensitive personal data may only be transferred outside of India where:<br>• The data principal provides explicit consent.<br>• The transfer is made pursuant to a contract or intra-group scheme approved by the DPA.<br>• The government has deemed a country or class of entities within a country to provide adequate protection.<br>• The DPA has specifically authorized the transfer.<br><br>Note there are narrow exemptions for preventing, investigating or prosecuting crime, enforcing legal rights and obtaining legal advice, and journalistic purposes, among others. | • Only sensitive data is subject to data transfer restrictions under the PDPB.[3]<br>• Even if these restrictions are overcome, a copy of the sensitive data must be retained in India.<br>• Although the PDPB envisions transfer mechanisms similar to the GDPR's safeguards, this would not eliminate the need to collect explicit consent.<br>• The PDPB does not provide a derogation for transfers that have been consented by the data principal without also requiring other mechanisms to be present. |

[3] However, note that the definition of sensitive personal data includes financial information. In addition, the Reserve Bank of India has promulgated requirements to localize payment data in India.

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| | Enforcement | | |
| PENALTIES | • The GDPR does not stipulate criminal liability, but permits member states to impose criminal penalties for violations of the regulation and applicable national rules.<br>• Administrative fines up to the higher of 20 million euros or a 4% of a group of undertakings' annual global revenue.<br>• DPAs may also issue injunctive penalties, which include the ability to block processing, restrict international transfers, and require the deletion of personal data.<br>• Individuals may bring claims in court for compensation and mechanisms exist for representative actions on behalf of a class of individuals. | • Imposes criminal liability on any person who, knowingly or intentionally, re-identifies personal data that has been deidentified by a data fiduciary or processor without that entity's consent by up to three years' imprisonment, a $3,000 fine or both, unless that person re-identifies their own data or if the relevant data principal has given their consent.<br>• Administrative fines up to the higher of approximately $2 million USD or a 4% of a group of companies' annual global revenue.<br>• The DPA may also issue injunctive penalties, which include the ability to block processing, restrict international transfers, and require the deletion of personal data.<br>• Individuals may bring claims to adjudicating officers appointed by the DPA for compensation and there is a mechanism to permit group actions. | • The penalty provisions under both regimes are similar, with the exception of the PDPB's criminal liability provisions, which are relatively narrow.<br>• One minor distinction is that the PDPB permits individuals to seek compensation from an administrative hearing before an adjudicating officer. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| Miscellaneous provisions | | | |
| ANONYMIZED DATA | • Although not defined by the GDPR, anonymous data, which cannot identify an individual by means reasonably likely to be used, falls outside of the scope of the law (reasonable steps to re-identify). In practice, anonymization is a high standard to meet. | • Anonymized data is data that has undergone an irreversible process of transforming or converting personal data to a form in which an individual cannot be identified, which meets the standards of irreversibility specified by the DPA.<br>• The government may, in consultation with the DPA, direct a data fiduciary or data processor to disclose anonymized data or other non-personal data "to enable better targeting of delivery of services or formulation of evidence-based policies" (S. 91(2)). | • The PDPB includes novel provisions that could require organizations to turn anonymized data over to the government. |
| SOCIAL MEDIA INTERMEDIARIES | • N/A. | • Social media intermediaries must enable the users who register their services from India or use their services in India to voluntarily verify their accounts in a manner prescribed by the government (S. 28(3)). Verified accounts would need to obtain a "demonstrable and visible mark of verification" (S. 28(4)). | • N/A. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| EXEMPTIONS FOR RESEARCH | • The GDPR permits a number of exemptions for scientific or historical research, archiving in the public interest, and statistical purposes, including:<br>  • Further processing for such purposes may be considered "compatible."<br>  • EU or member state law may permit controllers to process sensitive data for such purposes.<br>  • EU or member state law may provide derogations from certain individual rights.<br>• For the research exemptions to apply, controllers must implement appropriate safeguards, which may be specified by law, such as pseudonymization. | • The DPA may exempt a class or research, archiving or statistical processing from any provisions of the PDPB, if:<br>  • Compliance with the provision would disproportionately burden the purposes of processing.<br>  • The purpose cannot be achieved if the data is anonymized.<br>  • The data fiduciary has complied with a code of practice to be issued by the DPA on deidentification.<br>  • The personal data will not be processed in a manner that gives rise to significant harm or is used to take a decision concerning an individual. | • The PDPB research provisions allow for the possibility of wider exceptions than what is permitted by the GDPR, but much will depend on how these provisions are implemented by the DPA. |
| RULEMAKING AUTHORITY | • National DPAs and the EDPB are may issue guidance clarifying the application of provisions of the GDPR, but the guidance is non-binding.<br>• Some limited areas of the GDPR are left to national law, such as clarifying the conditions for processing criminal record data or adopting additional derogations from certain provisions. | • Many provisions either permit either the Central Government or the DPA to promulgate additional rules or regulations that may clarify PDPB requirements and/or specify additional requirements.<br>  • A complete list of areas where the Central Government is authorized to intervene is set out in Annex A.<br>  • A complete list of areas where the DPA is authorized to form additional rules, standards or regulations is set out in Annex B.<br>• The DPA may also develop codes of practice to aid organizations in complying. | • A significant number of provisions leave authority to the DPA to promulgate regulations that may affect important requirements.<br>• The Central Government has broad discretion to form policy, impose additional requirements, remove requirements from certain entities, and exercise control over the operation of the DPA. |

| TOPIC | GDPR | PDPB | ANALYSIS |
|---|---|---|---|
| APPLICATION TO PUBLIC AUTHORITIES | • The GDPR applies to public entities, subject to narrow exemptions:<br>  • Law enforcement and other "competent authorities" are subject to a separate, but similar framework where they are processing personal data for law enforcement purposes.<br>  • EU institutions are subject to a separate but similar framework.<br>  • Activities that fall outside the scope of EU law, such as national security and intelligence services, are subject only to national law. | • The PDPB generally applies to public agencies, as well as private parties.<br>• However, the Central Government has broad authority to exempt any government agency from any or all provisions in the interest of sovereignty, security, public order, integrity of the state and friendly relations with foreign states, or for preventing incitement of cognizable offences against the foregoing (S. 35). | • The PDPB grants the government broad authority to exempt itself and its agencies from any or all requirements.<br>• The purposes for which a government agency include "incitement" of offences against the state, which could conflict with rights of association and free expression. |


**Kurt Wimmer, CIPP/E, CIPP/US**

Partner and Co-Chair, Data Privacy and Cybersecurity Practice, Covington & Burling

**Gabe Maldoff,**

Associate, Covington & Burling

**Diana Lee,**

Law Clerk, Covington & Burling

# ANNEX A

## Powers of the Central Government

| | |
|---|---|
| S. 1(2) | The Central Government may decide the law's effective data and set different effective dates for different provisions. |
| S. 15(1) | The Central Government (in consultation with the DPA) may designate additional categories of sensitive personal data. |
| S. 26(4) | The Central Government may designate social media intermediaries as "significant data fiduciaries." |
| S. 33 | The Central Government may define "critical personal data," which is subject to the localization requirement. |
| S. 34(1)(b) | The Central Government (in consultation with the DPA) may designate a country, international organization or class of entities in a country as "adequate" for the purposes of transferring sensitive personal data. |
| S. 34(2)(b) | The Central Government may permit transfers of critical personal data where it determines the transfer does not affect India's security and strategic interests. |
| S. 35 | The Central Government may exempt any agency of the government from any or all of the provisions in the PDPB. |
| S. 37 | The Central Government may exempt any data processor or class of data processors, where the processor processes only data relating to individuals outside India pursuant to a contract with a person or entity outside of India. |
| S. 42(1) | The Central Government may appoint the chairperson and members of the DPA. |
| S. 44(1) | The Central Government has the authority to remove the chairperson and any member of the DPA. |
| S. 62(2) | The Central Government may specify the number of adjudicating officers, as well as the manner and terms of their appointment and their jurisdiction, among other requirements "as the Central Government may deem fit." |
| S. 64(8) | The Central Government may specify the procedure for hearing a complaint to the DPA. |
| S. 67(1) | The Central Government is tasked with establishing an Appellate Tribunal for appeals from the adjudicating officer. |
| S. 78 | The Central Government may appropriate to the DPA the amount of funds "as it may think fit for the purposes of this Act." |
| S. 86 | The Central Government may issue policy directions to the DPA "as it may think necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order." |
| S. 91(1) | The Central Government remains free to frame any policy for the digital economy that does not govern personal data. |
| S. 91(2) | The Central Government (in consultation with the DPA) may direct any data fiduciary or data processor to disclose any anonymized data or other non-personal data. |
| S. 92 | The Central Government may prohibit a data fiduciary from processing biometric data. |
| S. 93(1) | The Central Government may make rules to carry out the provisions of the PDPB. |
| S. 97(1) | The Central Government may remove any inconsistencies "as may appear to be necessary or expedient." |

# ANNEX B

## Areas Where Discretion Is Accorded to the DPA

| | |
|---|---|
| S. 3(2) | The DPA may establish standards of anonymization. |
| S. 7(1)(n) | Regulations may specify additional information that must be included in privacy notices. |
| S. 9(4) | Regulations may specify how personal data must be deleted when it is no longer required. |
| S. 14(1) | Regulations may specify "reasonable purposes" for processing personal data without consent, which take into account a number of listed factors. Where the DPA establishes reasonable purposes, it must also set out safeguards for such processing. |
| S. 15(2) | The DPA may (by regulations) specify additional safeguards or restrictions for processing sensitive personal data. |
| S. 16 | The DPA may (by regulations) specify how to conduct age verification of children, how to obtain parental consent, when a data fiduciary will be classified as a "guardian data fiduciary," and how the children's provisions will apply to counselling and child protection services. |
| S. 17(3) | Regulations may specify how to comply with the access right. |
| S. 18 | Regulations may specify how to comply with correction and erasure requests. |
| S. 21 | Regulations may specify the time period for responding to a request and any fees that may be charged. |
| S. 22(2) | The DPA may (by regulations) specify a process for obtaining certification of a privacy-by-design policy. |
| S. 23(1) | Regulations may provide further detail on transparency requirements. |
| S. 24(2) | Regulations may specify how to comply with information security requirements. |
| S. 25(3) | Regulations may specify the time period for reporting breaches. |
| S. 26 | The DPA may notify a data fiduciary (or class thereof) as a significant data fiduciary based on factors enumerated in the PDPB. The DPA may also classify significant data fiduciaries, notwithstanding the enumerated factors, where it considers there to be a significant risk of harm. |
| S. 27(2) | The DPA may (by regulations) specify the circumstances where a DPIA would be required and where a data auditor may be required to conduct the DPIA. |
| S. 28(1) | Regulations may specify the form and manner of maintaining records of processing. |
| S. 29(3) | The DPA shall (by regulations) specify the form and procedure for conducting data audits. |
| S. 29(6) | The DPA shall (by regulations) establish the criteria for assigning a data trust score. |
| S. 29(7) | The DPA may direct any data fiduciary to conduct an audit where a processing activity is likely to cause harm, even if other criteria are not met. |
| S. 34(1)(c) | The DPA may permit the transfer of any sensitive personal data or class of such data outside of India for any specific purpose. |
| S. 38 | The DPA may exempt certain classes of processing for research, archiving or statistical purposes from provisions of the PDPB, where it is satisfied that a series of enumerated criteria are met. |
| S. 39(2) | The DPA may (by regulations) define "small entities" that will be exempt from some requirements of the PDPB. |

S. 50 The DPA shall produce codes of practice to promote effective data protection, which may include the following topics:

- Transparency requirements.
- Data quality and storage limitation.
- Consent and other lawful bases (including "reasonable purposes").
- The grounds for processing sensitive personal data.
- Processing of children's data.
- Individual rights.
- Accountability requirements.
- Information security and data breach response.
- Deidentification and anonymization.
- Methods of deletion, destruction or erasure.
- International transfers.
- Processing for research, archiving or statistical purposes.
- Any other matter it determines is necessary.

S. 94(2) The DPA may make regulations on any or all of the topics indicated above or any other topic consistent with the PDPB.