The Sections of Antitrust Law and International Law (“the Sections”) of the American Bar Association respectfully submit these comments on the Personal Data Protection Bill, 2019 (the “PDPB”), which was referred to the Joint Committee on The Personal Data Protection Bill (the “Committee”) of the Parliament of India (“Parliament”). The Sections previously commented on the White Paper of the Government of India Committee of Experts and the Ministry of Electronics and Information Technology (the “White Paper”), and we very much appreciate the opportunity to comment on the PDPB as well. We applaud Parliament for moving forward with draft legislation in this critically important area of the law, as well as the improvements that have been made in the PDPB compared to the 2018 draft.

These comments are intended to further this dialogue and reflect the Sections’ experience in international and cross-border privacy and data security issues. Although we are not experts in the law of India, the Sections’ long involvement in these issues rests on the participation of both private and public sector lawyers, economists, and market participants, reflecting the interests of all those who engage in, benefit from, and enforce legal rights relating to, digital as well as traditional commerce in which personal data plays an important role. The Sections do not advocate on behalf of any particular interest or party; rather, we offer our comments as constructive input that we hope will be useful to the Committee.

In these Comments, the Sections make several suggestions that we believe both further the goals of modernization in the areas of privacy and data security and global harmonization and serve the desired balance between individual privacy and the development of information markets and services that benefit Indian nationals, the Indian economy and the development of a global marketplace.

Executive Summary

The Sections’ comments make the following suggestions:

- **Data Localization.** We applaud the Committee for its creative approach to balancing the needs expressed by the Indian government on the need for data to be localized within India with the needs expressed by global industry for a more flexible approach. However, the PDPB’s data localization framework is likely to harm Indian businesses, including start-ups and SMEs, which


will be denied the ability to participate in global data storage. It also may hinder the India from achieving its ambitious vision of urban revitalization through its Smart Cities initiative, without any corresponding tangible benefits to the sector or Indian citizens. Accordingly, we reiterate our prior recommendation to remove data localization provisions from the PDPB.

- **Grounds for Processing:** We make two suggestions on grounds for processing data:
  
  - First, we suggest that the “reasonable purpose” ground for processing be revised to more closely align to the “legitimate interest” ground for processing under the General Data Protection Regulation (“GDPR”) of the European Union (“EU”). In particular, we suggest that the data fiduciary document the reason for processing, as the PDPB would require, but that the decision on whether processing will be permissible be made, in the first instance, by the data fiduciary rather than the Data Protection Authority (“DPA”). Without this change, the DPA will be inundated by requests for approval of “reasonable purpose” requests, and commerce in India will be obstructed by the need for government approval prior to moving forward with commercial processing.
  
  - Second, we suggest that the PDPB include processing to fulfill a contract as legitimate processing, which is a feature of the GDPR and most global privacy laws. This improvement would permit Indian e-commerce to work more smoothly for the benefit of consumers and companies alike.

- **Involvement of the Central Government in Key Capacities.** In several areas of the PDPB as compared to the 2018 draft bill, the drafters have moved decisionmaking authority from the DPA to the Central Government. This change fundamentally alters the nature of the decisions that may be made, whether these decisions relate to the definition of “sensitive personal data” or other equally important aspects of privacy regulation. The DPA is a superior decisionmaking body, given that it will be broadly representative and will develop extraordinary expertise in data privacy. In addition, vesting this discretion in the executive branch of government is likely to frustrate India’s opportunity to obtain a determination of adequacy from the EU, which would create highly favorable data flows between India and the EU.

- **Disclosure of Specific Sharing Arrangements to Data Principals.** Section 17(3) provides that data principals have the right to access the identities of the data fiduciaries with whom personal data has been shared by any data fiduciary. We believe that this section could be readily used by competitors to obtain competitively sensitive information, and would fail to provide actionable information to data principals. We suggest that disclosure be made of the categories of companies with which data is shared, rather than the actual identity of those companies.

- **Definitions of Categories of Personal Data.** Given the importance of the definitions of “sensitive personal data” and other categories of personal data, we suggest improvements for the Committee’s consideration.

- **Profiling and Automated Decision-Making.** The PDPB recognizes the need for and provides protection from automated and significant decisionmaking to data subjects or data principals who are deemed children. We suggest the Committee consider adding a provision to the PDPB to provide safeguards for all data principals in relation to automated decisionmaking.

- **Application to the Processing of Data of Foreign Nationals.** We appreciate that the PDPB empowers the Central Government to except the processing of foreign nationals, but we would suggest that the scope of the PDPB provide clearly that it is not applicable to foreign national data being processed in India under a contract.
• **Period for Compliance.** The PDPB will create one of the world’s most significant data protection regimes, and will require entirely new mechanisms and obligations. As was the case with the GDPR and other significant changes in data protection law and policy, we suggest that the Joint Committee include a grace period to come into compliance of at least three years.

We appreciate the opportunity to provide commentary to Parliament and would be pleased to continue our participation or respond to any comments or inquiries that may be useful during this process.

**Specific Suggestions**

1. **Data Localization**

Unlike the GDPR or any other generally applicable privacy law globally, the PDPB contains mandatory data localization provisions. The PDPB restricts cross-border transfers of both sensitive personal data and “critical personal data,” but does not impose limitations on outward transfers of personal data that do not fall into these categories. In brief:

- **Sensitive Personal Data:** Sensitive personal data may not be transferred outside of India unless the data principal gives explicit consent and one of the following conditions is satisfied: (1) the transfer is made pursuant to a contract or intra-group scheme approved by the DPA; (2) the government has deemed a country or class of entities within a country to provide adequate protection; or (3) the DPA has specifically authorized the transfer. Even if the data fiduciary satisfies an exemption, the entity must retain a copy of the sensitive personal data in India.

- **Critical Personal Data:** “Critical personal data” must be processed only in India, except under emergency circumstances or where the government has approved the transfer, taking into account India’s security and strategic interests. The PDPB gives the Government broad discretion to define “critical personal data” and does not specify limiting criteria.

- **Personal Data:** The PDPB does not contain restrictions on cross-border transfers of personal data that are not sensitive or critical personal data.

The Sections reiterate concerns expressed previously regarding the negative impact of data localization laws and rules that limit the storage, movement, or processing of data. In particular, we are concerned that Section 33 of the PDPB would require all “sensitive personal data” to be stored on a server in India, and that Sections 33 and 34 would prohibit the transfer of “critical personal data” outside of India and allow its processing in India only under limited circumstances. Given that the definition of “sensitive personal data” includes some day-to-day financial elements, this restriction could greatly hamper cross-border commerce.

In today’s rapidly changing digital ecosystem, it may be tempting to cite the protection of personal data and ensuring data security as reasons for imposing data localization requirements. However, while we agree that data security and privacy are of paramount importance, we do not embrace the approach outlined in the PDPB. Indeed, potential privacy and security risks may be heightened due to the PDPB’s data transfer and data localization requirements.

As previously noted, data localization may be a trade barrier and raise barriers to entry for cross-border competitors since the security of data depends on the administrative, physical, and technical safeguards that are put in place to protect the confidentiality, integrity, and availability of the data. Data localization also may lead to mirroring of data in multiple jurisdictions. This outcome conflicts with data minimization and may create additional potential sources of data compromises.
Because lowering barriers to data transfers across national borders plays a critical role in the development of innovative technologies and digital goods and services, as well as contributes to the growth of the broader economy, India’s enterprises could also benefit from open and flexible data privacy frameworks. Indeed, businesses of all sizes, including Indian startups and SMEs as well as larger Indian businesses with international operations, are able to thrive when they leverage global cloud platforms and face limited barriers to entry as they expand and conduct business in global markets. The PDPB data localization framework also is inconsistent with the Government of India’s ambitious vision of urban revitalization by developing 100 mid-sized Smart Cities with high-tech capabilities to enhance performance and well-being, while reducing costs and resource consumption, in order to engage more effectively and actively with citizens. Instead, the proposed PDPB data localization framework would impose substantial costs on India’s small tech start-ups, without any corresponding tangible benefits to the sector or Indian citizens.

To overcome the challenges associated with the aforementioned PDPB data localization provisions, we believe that a data protection enforcement agency, with flexible authority, coupled with international enforcement cooperation and a self-regulation framework would appropriately address data protection issues and achieve maximum compliance. For example, the FTC is the main U.S. privacy agency, focusing on commercial consumer privacy issues. Although the FTC does not enforce laws that govern cross-border data flows, Section 5 of the FTC Act (and its 2006 amendment, the U.S. SAFE WEB Act), provides the FTC with the authority to investigate and prevent abuses of personal data as an issue of consumer protection and substantive data protection (under its authority to investigate “unfair and deceptive acts or practices”) and to cooperate on international enforcement cases.

The Sections therefore recommend deleting Sections 33 and Section 34, which contain the aforementioned cross-border data transfers and data localization restrictions. This would provide the PDPB with a more flexible framework, which could evolve over time to take account of technological developments, increased global data flows, international enforcement cooperation and at the same time foster the growth of local Indian companies and the interests of global entities considering doing business in India.

2. Grounds for Processing Personal Data

"Reasonable Purpose" Grounds for Processing. Section 14 of The PDPB provides that “personal data may be processed without obtaining consent under section 11 if “such processing is necessary for such reasonable purposes as may be specified by regulations” to be promulgated by the new Data Protection Authority (“DPA”). In promulgating those regulations the DPA should take into account: “(a) the interest of the data fiduciary in processing for that purpose; (b) whether the data fiduciary can reasonably be expected to obtain the consent of the data principal; (c) any public interest in processing for that purpose; (d) the effect of the processing activity on the rights of the data principal; and (e) the reasonable expectations of the data principal having regard to the context of the processing.” Examples of "reasonable purposes" “may include— (a) prevention and detection of any unlawful activity including

---

3 Given that India’s small enterprises are vital to India’s Smart Cities goal of a modern economy, this is likely a fatal flaw. If the data localization provisions are implemented, small Indian companies would face uncertainty and unforetold compliance costs in connection with the new overly rigid data localization standards outlined in the PDPB.

4 Section 11 (1) provides that “The personal data shall not be processed, except on the consent given by the data principal at the commencement of its processing.”

5 Section 14(1).
fraud; (b) whistle blowing; (c) mergers and acquisitions; (d) network and information security; (e) credit scoring; (f) recovery of debt; (g) processing of publicly available personal data; and (h) the operation of search engines.\textsuperscript{6} Even if a reasonable purpose is found, the DPA “shall— (a) lay down, by regulations, such safeguards as may be appropriate to ensure the protection of the rights of data principals; and (b) determine where the provision of notice under section 7 shall apply or not apply having regard to the fact whether such provision shall substantially prejudice the relevant reasonable purpose.”\textsuperscript{7}

The EU Union permits several grounds for lawful processing of data including if it is necessary for purposes of “legitimate interests.”\textsuperscript{8} Under the EU approach, the data controller/data fiduciary determines whether it applies. As explained by the UK ICO, there are three elements to the legitimate interests basis:\textsuperscript{9}

- Identify a legitimate interest -- The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits [this roughly corresponds to Section 14(1)(a)]
- Show that the processing is necessary to achieve it -- If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply [this roughly corresponds to Section 14(1)(b)]; and
- Balance it against the individual’s interests, rights and freedoms -- If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests [this roughly corresponds to Section 14(1)(d)].

This analysis must be documented by the data controller.

The key differences between the EU and Indian approach, and the impact on India if the current version of the draft is adopted are as follows:

First, in the EU, prevention of fraud, ensuring network and information security and indeed all the categories set out in Section 14(2), is presumptively, if not always, a legitimate interest. \textsuperscript{10} Inclusion

\textsuperscript{6} Id.

\textsuperscript{7} Section 14(3)

\textsuperscript{8} Article 6(1). Other exceptions include if it is necessary to perform a contract with the data subject or to comply with various legal obligations/protect the vital interests of a data subject/is in the public interest.


\textsuperscript{10} The EU explicitly states that “Your company/organisation has a legitimate interest when the processing takes place within a client relationship, when it processes personal data for direct marketing purposes, to prevent fraud or to ensure the network and information security of your IT systems.” https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en. Relying on Article and Recitals (47), (48) and (49) of the GDPR and Article 29 Working Party Opinion 06/2014. Thus Recital (47) provides that “Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller ... the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. [This roughly corresponds to Section 14(1)(e).] ... The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The
in the PDPB of the word “may” for the instances specified in Section 14(2) and the inclusion of exceptions even then under Section 14(3) simply creates the concern that the DPA regulation will put those doing business in India at risk of fraud or network security threats because processing personal data to prevent either would be an “unreasonable purpose.” Any concern that relevant negative personal data relating to fraudulent behavior or credit fraud may not be processed, will deter others from extending credit, investing or otherwise doing business with Indian nationals and small or medium Indian businesses (SME’s). To overcome this, the Sections suggest that all the categories enumerated in Section 14(2) be designated as “reasonable purposes.”

Second, reasonable purposes such as processing personal data within a client relationship, or for direct marketing purposes, identified by Europe as legitimate interests, are not even mentioned in the PDPB. Failure of the DPA to address these purposes in their regulations because they were not mentioned in section 14(2) means that such legitimate uses may require consent under section 11 even though the factors identified in section 14(1) may be satisfied.

And this goes to the final issue: DPA determination of “reasonable purpose” versus self-determination. Anticipated purposes in a regulation issued by the DPA would not include unforeseen purposes that emerge in the future or that did not appear significant enough to merit inclusion in the regulation. Even for those purposes that are addressed in any regulation, the fact specific nature of each use suggests that no regulation can fully address the virtually unlimited ways in which processing personal data for a reasonable purpose can arise and so will be under- or over-inclusive. A business could petition the DPA to validate an unanticipated or unaddressed reasonable purpose but (i) disclosure in public proceeding would compromise their intellectual property or first to market advantage; (ii) to the extent such a review would take time would discourage applications where products have very quick life cycles; and (iii) any decision to incur the likely significant expense of petitioning the regulator, would also be based on an assessment of the likelihood of success, with any doubt resulting in a decision not make such an application. All these considerations will materially and negatively impact innovative uses of personal data in India. The uncertainty of the regulatory process means businesses will avoid innovative and useful applications that they might have implemented if they could make a self-determination of legitimate use, as they can do in the EU. The data controller, in good faith and documenting its determination, is better situated to make that analysis, subject to regulatory oversight after the fact.

Processing to Fulfill a Contractual Request. Data processing requirements in the EU and most global privacy regimes permit several grounds for lawful processing of data, including when necessary to perform a contract with the data principal. See GDPR Art. 6(1)(b). The PDPB, in contrast, excludes this ground for lawful processing and focuses on requiring a separate consent from the data principal, even in the case where the processing is at the request of the data principal for the performance of a contract to which the data principal is a party. The Sections believe that excluding this common-sense ground for lawful processing will result in unnecessary and legalistic consent requirements that consumers will neither expect nor appreciate. True consent is undermined when consumers experience “consent fatigue” and simply check “accept” to move through a transaction or signup without meaningfully reviewing options before providing consent. For this reason, other bases for processing are often permitted when they are in the reasonable expectations of the consumer. In the United States, the Federal Trade Commission (“FTC”) has recognized that affirmative express consent should be required

processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.”
only when the particular use of data would be unexpected by the consumer. Performance of a contract, at the request of the data principal, is a context in which the consumer will fully expect that data will be processed, given that the data principal has commenced the transaction. Accordingly, we recommend that contractual grounds for processing be included in the PDPB in a manner that is generally consistent with the GDPR.

Proposed Modifications:

12. Notwithstanding anything contained in section 11, the personal data may be processed if such processing is necessary,—

* * *

(g) for the performance of a contract to which the data principal is a party or in order to take steps at the request of the data principal prior to entering into a contract.

* * *

14. (1) In addition to the grounds referred to under sections 12 and 13, the personal data may be processed without obtaining consent under section 11, if such processing is necessary for such reasonable purposes as may be specified by regulations determined by the data fiduciary, after taking into consideration—

(a) the interest of the data fiduciary in processing for that purpose;

(b) whether the data fiduciary can reasonably be expected to obtain the consent of the data principal;

(c) any public interest in processing for that purpose;

(d) the effect of the processing activity on the rights of the data principal; and

(e) the reasonable expectations of the data principal having regard to the context of the processing.

(2) For the purpose of sub-section (1), the expression "reasonable purposes" may include—

(a) prevention and detection of any unlawful activity including fraud;

(b) whistle blowing;

(c) mergers and acquisitions;

(d) network and information security;

(e) credit scoring;

(f) recovery of debt;

(g) processing of publicly available personal data; and

(h) the operation of search engines; and

(i) when the processing takes place within a client relationship.

For the purpose of sub-section (1), the expression "reasonable purposes" may also include other purposes including processing personal data for direct marketing purposes.

Where the Authority specifies a reasonable purpose under sub-section (1), it shall—

(a) lay down, by regulations, such safeguards as may be appropriate to ensure the protection of the rights of data principals; and

(b) determine where the provision of notice under section 7 shall apply or not apply having regard to the fact whether such provision shall substantially prejudice the relevant reasonable purpose.

3. The Role of the Central Government Under the PDPB

Substituting the DPA for the Central Government. In several areas of the PDPB, the drafters have entrusted decision-making authority to the Central Government. This is a change from the 2018 draft bill, which generally reserved decision-making authority to the DPA, and is very unusual among recent data protection legislative efforts around the world. This change fundamentally alters the nature of the decisions that may be made, whether these decisions relate to the definition of “sensitive personal data” or other equally important aspects of privacy regulation, by removing these decisions from the expert agency and putting them squarely in the purview of elected politicians.

Based on the Sections’ experience in reviewing global data protection laws, this level of involvement of the Central Government in the operation of the privacy regulatory scheme envisioned by the PDPB would be unusual. Because data protection authorities tend to be expert agencies, data protection laws around the world generally leave decisions such as these to the agency rather than the executive branch of government. In India, the DPA would be a superior decision-making body for the complex and intricate decisions relating to data privacy, particularly given the many languages and geographies of India. The DPA will be broadly representative of these diverse populations and areas and will develop exceptional expertise in the data privacy issues that are unique to India.

Finally, vesting decision-making ability in the executive branch of government is likely to frustrate India’s golden opportunity to obtain a determination of “adequacy” from the EU. A key requirement for a finding of “adequacy” is a finding that key regulatory decisions are made by an independent regulator and not by the executive branch of government. A finding of adequacy would create highly favorable data flows between India and the EU if it could be determined that India’s system of data protection is “adequate” to the system under the GDPR.

To resolve this issue, we suggest substituting “the Authority” for “the Central Government” in the following sections. An alternative approach would be to commit these decisions to “the Authority, after consultation with the Central Government” if the Committee wishes to ensure consultation:

- Section 3(36): The Central Government may create additional categories of “sensitive personal data.

---

12 See European Comm’n Implementing Decision (EU) 2019/419 of 23 January 2019, 2019 O.J. (L 76) 1 (In approving an adequacy decision for Japan, the European Commission noted that “an independent supervisory authority tasked with powers to monitor and enforce compliance with the data protection rules should be in place. This authority should act with complete independence and impartiality in performing its duties and exercising its powers”).
• Section 33(2): The Central Government has sole responsibility for defining the concept of “critical personal data,” which is important for the operation of the PDPB’s data localization regime.

• Section 35: The Central Government may create an exception from any part of the PDPB from applying to any agency of the government.

• Section 37: The Central Government has sole authority to exempt companies from the application of the PDPB if they are processing data from outside of India.

• Section 92: Data fiduciaries may only process the types of biometric data that are authorized by the Central Government.

Government Requirements for Submission of Data. Section 91(2) of the PDPB provides that the Central Government can direct any data fiduciary or data processor to submit to the Government any anonymized or other non-personal data for the use of the Government itself. This is a highly unusual provision that requires the private sector to surrender significant amounts of data to the government. To the extent that personal data provided to the government might not have been securely anonymized, this provision could result in significant data security issues in India. Rather than substitute the Authority for the Central Government in this provision, the Sections suggest that this provision be deleted from the PDPB.

4. Disclosure of Specific Sharing Arrangements in Data Subject Access Requests

Section 17(3) provides that “The data principal shall have the right to access 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, in such manner as may be specified by regulations.” Two issues are raised:

First, providing the specific identities of the other data fiduciaries may discourage the use of personal information for reasonable purposes under the PDPB. For example, a data fiduciary seeking personal information for network and information security purposes may not want this specific fact disclosed to the data principal, who then would be aware that their conduct is of concern and may seek to circumvent measures taken by a data fiduciary to protect a network from unauthorized intrusion by that data principal.

Second, disclosure of each data fiduciary may lead to the disclosure of proprietary customer lists and other competitively sensitive information. A competitor who is also a data principal could abuse the process to identify its competitor’s customers and business partners. It would be best to conform the first part of this sub-section “categories of data fiduciaries” to the second part of this subsection “categories of personal data.”

Proposed Modifications to the language of Section 17(3):

“The data principal shall have the right to access in one place the identities categories 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, in such manner as may be specified by regulations.”

5. Definitions of Certain Data Categories

The PDPB appropriately differentiates among different kinds of data, including “personal data,” “anonymized data,” and “sensitive data.” We provide some suggestions for modification of their scope and language based on analogous privacy laws. We also discuss the addition of the category of “critical personal data.”
The draft legislation defines “personal data” as “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.” We suggest that the definition could be amended to require that the data be “reasonably linked to an individual.” The GDPR similarly defines “personal data” as “any information relating to an identified or identifiable natural person,” and adds “an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier.”

Similarly, the U.S., the Federal Trade Commission views “personal data” as data that can be “reasonably linked” to a specific individual or device. Both incorporate a concept that data is “personal” only if a specific person can be reasonably identified by that data. Data that cannot be reverse-engineered to link to an individual would not be covered.

Likewise, anonymized data appropriately falls outside of the definition of “personal data” because such data can no longer reasonably identify a particular individual. We therefore suggest that the law be clear that anonymized data is excluded from personal information by definition. In the PDPB, the definition of “personal data” could be amended to exclude “anonymized” data, and the definition of “anonymization” could refer to data generally, not to “personal data.”

Additionally, the current proposed definition requires that “anonymization,” which is a component of “anonymized data,” be an “irreversible process” that meets a standard of “irreversibility” specified by the DPA. “Irreversibility” is far too high a standard, and is well outside the mainstream. We suggest that the standard focus more on whether the data effectively may be re-linked to an individual using “reasonable efforts,” rather than a “irreversibility” that may be interpreted overly strictly. Recital 26 of the GDPR refers to “anonymous information,” to which data protection principles do not apply, as “data rendered anonymous in such a way that the data subject is not or no longer identifiable.” In assessing whether means are reasonably likely to be used for re-identification, “account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.” In the United States, the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) Privacy Rule provides two methods for de-identifying personal data (the Expert Determination Method and the Safe Harbor method). Additionally, contractual limitations may be an effective way of limiting re-identification anonymized data in an enforceable way. These kinds of alternatives will avoid setting a standard that may be viewed as impossible to meet even for data that is, by reasonable measures, effectively de-identified in a manner that will protect Indian data principals.

The proposed legislation also includes a definition of “sensitive personal data,” which lists specific categories of information that is subject to higher protections, and also permits the Central Government, in consultation with the Authority and the sectoral regulator, to designate additional information as “sensitive.” We suggest that a fact-based approach, focused on predictions of actual harm, be considered by the Joint Committee. The current draft does recognize “the risk of significant harm that may be caused to the data principal” and “whether a significantly discernable class of data principals may suffer significant harm” as two factors in identifying additional categories of sensitive

13 GDPR Article 4(1).

data, along with the expectation of confidentiality and the adequacy of protections afforded to non-sensitive data. Although this approach provides some guidance for future action, it creates significant uncertainty for stakeholders. Article 9 of the GDPR, in contrast, contains a specific list of “special categories of personal data.” The U.S. has established specific rules for certain kinds of data, such as health information under HIPAA. The possibility of the government creating additional categories of sensitive information without additional legislation – which would trigger heightened obligations – will make the scope of the law less predictable and make compliance more difficult. We suggest consideration of limiting the categories of sensitive information to those specified in the legislation, or providing a more predictable and constrained process, involving stakeholder input, for determining whether additional categories of data will be deemed “sensitive” and subject to heightened protections.

Finally, the draft legislation identifies a new category of “critical personal data,” which is defined as “personal data as may be notified by the Central Government to be critical personal data.” It further provides that critical personal data may be processed only in India, with limited exceptions, including where the Central Government concludes that transfer “does not prejudicially affect the security and strategic interest of the State.” As noted above, the localization provisions of the draft legislation can create significant impediments to outside business investment. The discretion provided to the Central Government to designate “critical personal data,” combined with the lack of standards around such designations, creates substantial uncertainty and would further constrain business involvement. This kind of “critical data” does not have parallels in the GDPR or U.S. privacy law, and instead appears to be related to national security concerns. We suggest that the undefined concept of “critical personal data” be removed from the draft privacy legislation, to provide greater predictability for all stakeholders.

6. Automated Decision-Making

The PDPB includes several definitions and a substantive section on automated decisionmaking, which generally refer to artificial intelligence or machine learning. Section 3(6) defines “automated means” as “any equipment capable of operating automatically in response to instructions given for the purpose of processing data.” Sections 19(1) provides a right to data portability and access for data principals when data has been processed through automated means:

“Where the processing has been carried out through automated means, the data principal shall have the right to receive the following personal data in a structured, commonly used and machine-readable format the data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained,” and “have personal data referred to in clause (a) transferred to any other data fiduciary in the format referred to in that clause.”

Transparency in terms of data portability is an important first step. In the Sections’ view, a workable approach was that taken by the Article 29 Working Party in its Guidelines on Automated individual decisionmaking and Profiling for the purposes of Regulation 2016/679 (the “Guidelines”). The Guidelines provide that a controller making automated decisions must “tell the data subject that they are engaging in this type of activity; provide meaningful information about the logic involved; and explain the significance and envisaged consequences of the processing.” The European Data Protection

---

Board (the “EDPB”), which replaced the Article 29 Working Party under the GDPR, also endorses the Guidelines. ¹⁶

Accordingly, the right to access the logic behind automated decisionmaking, even where technically complex, is guaranteed in a meaningful and understandable way for data subjects or data principals. The Sections note that the GDPR defines the universe of automated decisionmaking subject to its rule in Article 22(1) as “a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.” The Sections suggest a materiality limitation in line with the GDPR approach and believes that adopting the transparency requirements identified in the Guidelines supported by the EDPB is a sound solution to automated decisionmaking and profiling.

7.  **Excluding Data Processing of Foreign Nationals by Contract**

India’s outsourcing industry, without question, leads the world. The Indian government estimates that the outsourcing sector contributes more than $52 billion to India’s economy. ¹⁷ This industry sector is important not only to India, but to countries around the world.

The Sections appreciate the PDPB’s inclusion of Section 37, which permits the Central Government to issue decisions creating exceptions to the terms of the PDPB for certain industries. But this approach, which may operate on an industry-by-industry or even company-by-company basis, may undermine global industry confidence in India’s outsourcing industry. Accordingly, we suggest that this industry simply be carved out across the board, given that it does not involve the processing of the personal data of Indian data principals at all and does not implicate the goals of the PDPB.

To accomplish this change, Section 37 could be amended as follows:

37. The Central Government may, by notification, exempt from the application of this Act, shall not apply to the processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law.

8. **Compliance Period**

The PDPB, when enacted, will require thousands of companies to create new data maps and mechanisms for compliance. Some multinational companies may already have done some work to comply with GDPR and other statutory schemes, but this work will be entirely new for many companies and industries. And even for companies that have adopted compliance plans for GDPR, the PDPB has many key substantive differences from the GDPR that will require significant new compliance efforts.

On the government side, the establishment of the DPA under the PDPB will require significant effort and time to accomplish.

In the case of major changes from the EU to Brazil, countries permit relatively lengthy periods for compliance, recognizing the scope of business changes that will be required by the legislation. The GDPR permitted just under two years for coming into compliance prior to its effective date, even though GDPR was essentially an evolution of requirements from the EU Data Protection Directive 1995. In Brazil, the Lei Geral de Proteção de Dados Pessoais (“LGPD”), which is similar in scope to the GDPR, anticipated two years for a period for industry to come into compliance, and in practice that period may

---


be extended. Given the scope of the PDPB and the extent of the changes that will be required, the Sections recommend a period of at least three years after passage before its provisions come into force.

**Conclusion**

The Sections appreciate the opportunity to comment on the Personal Data Protection Bill, and commend the Joint Committee of Parliament for this open and transparent process. If the Sections can clarify or expand upon any of the matters discussed herein or answer any questions, we would be pleased to do so.