21 February 2020

Comments by the Centre for Information Policy Leadership on India's Personal Data Protection Bill 2019

The Centre for Information Policy Leadership (CIPL)[1] welcomes this opportunity to provide comments to the Joint Parliamentary Committee on Bill No. 373 of 2019, the Personal Data Protection Bill (PDPB), as introduced in the Lok Sabha on 11 December 2019.[2]

CIPL has previously provided extensive comments to the Ministry of Electronics and Information Technology (MeitY) on the Draft Personal Data Protection Bill 2018[3] and stands by those recommendations, many of which are still of relevance and applicable to the PDPB 2019. CIPL strongly recommends that the Joint Parliamentary Committee revisit these previous comments as it reviews the PDPB 2019. A copy of the comments can be found here: https://bit.ly/376cg8E.

CIPL's comments below reiterate several of its previous recommendations which it believes are of critical importance for the Joint Parliamentary Committee to consider during its review of the Bill.

Summary of CIPL Key Recommendations

1. **Extraterritorial Scope:** Refine the PDPB's extraterritoriality provision to ensure the law extends only to data fiduciaries located outside of India that specifically direct their services to Indian residents and purposefully collect personal data of Indian residents.

2. **Anonymization:** Revise the definition of anonymization to reflect the more realistic standard of reasonable anonymization coupled with procedural, legal and administrative safeguards and account for the need to re-identify data in certain circumstances for the benefit of individuals.

3. **Processing Data for Employment Purposes:** Revise the provision on processing of personal data necessary for purposes related to employment to permit the processing of sensitive data for such purposes. Sensitive data, such as financial and health data, are often processed to pay salaries, arrange health insurance, etc.

4. **Reasonable Purposes:** Revise the scope of the reasonable purposes processing ground, in line with the concept of legitimate interest in other global privacy laws. Ensure that reasonable purposes is

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] India Personal Data Protection Bill No. 373 of 2019, as introduced in the Lok Sabha on 11 December 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[3] See CIPL Comments on the Indian Ministry of Electronics and Information Technology's Draft Data Protection Bill 2018, 26 September 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_indian_ministry_of_electronics_and_information_technology%E2%80%99s_draft_data_protection_bill_2018.pdf.

placed on an equal footing with consent and not treated as a residual processing ground where consent is not feasible.

5. **Personal Data Breach:** Notification to the data protection authority should occur "without undue delay" after the data fiduciary has awareness and sufficient information about the nature of the breach. Notification to data principals should be a decision of the data fiduciary (rather than the data protection authority) if the breach is likely to result in a high risk or significant harm to individuals.

6. **Significant Data Fiduciaries:** Remove the concept of "Significant Data Fiduciaries" from the PDPB. The standard for compliance with obligations applicable to significant data fiduciaries should be laid out in their respective sections.

7. **Data Protection Officer:** There should be no specific location requirement for the data protection officer. At most, the law should follow the GDPR model of requiring a legal representative of the data fiduciary in India.

8. **Prohibition on Processing Sensitive and Critical Personal Data Outside of India:** Remove the local processing and storage requirements for sensitive and critical personal data and protect such data as it flows outside of India via adequacy findings or technical and legal measures, such as contracts and accountability-based frameworks (e.g. enforceable corporate rules, codes of practices, codes of conduct and certifications).

9. **Conditions for the Transfer of Sensitive and Critical Personal Data:** Revise the PDPB to permit transfers of sensitive personal data outside of India via contracts, intra-group schemes or adequacy decisions without additionally requiring explicit consent on top of such protective measures. Reserve explicit consent as a means for transferring data where such alternative protections are not available. Define critical personal data narrowly to avoid unintended categories of data being limited to transfer under extremely narrow exceptions.

10. **Power of Central Government to Exempt Certain Data Processors:** Clarify that the exemption in the PDPB also applies to the processing of sensitive personal data of data principals outside of India and expand the current provision to expressly exempt global service centers from the application of the Act where such centers process personal data of data principals outside of India.

11. **Codes of Practice:** Broaden the provision on Codes of Practice to also include privacy seals, marks and certifications which would provide additional domestic compliance tools as well as tools for cross-border data transfers.

12. **Direction to Share Anonymized and Non-Personal Data with the Central Government:** Remove the provision permitting the central government to request anonymized personal data or other non-personal data from data fiduciaries and processors to enable better targeting of delivery of services or formulation of evidence-based policies. While CIPL supports accountable data sharing between organizations in the public and private sectors for social good, such sharing should be the subject of a separate discussion and not included as a provision in the PDPB.

13. **Timeline for Adoption:** Specify in the PDPB or by notification in the Official Gazette a reasonable, realistic and sensible effective date for the PDPB of at least two years from its passage and/or the establishment of a fully functional data protection authority to give organizations and the data protection authority of India adequate time to prepare for the new rules.

Comments

Section 2: Application of Act to processing of personal data

Currently, the PDPB applies to processing of personal data (1) collected, disclosed, shared or otherwise processed in India (2) processed by the State, any Indian company, citizen or persons/body of persons incorporated or created under Indian law or (3) by data fiduciaries or processors outside of India if the processing is in connection with any business carried on in India, systematic activity of offering of goods or services to data principals in India or profiling of data principals in India.

CIPL believes that the wide scope and cumulative application of this provision will lead to several issues including conflicts of law with other data privacy laws (e.g. in cases where a processor processes data on behalf of a foreign data fiduciary and there are conflicts between the foreign privacy law and the PDPB) and the indirect application of the PDPB to foreign data fiduciaries by virtue of their relationship with foreign service providers that outsource work or otherwise transfer data to a processor in India (e.g. where a Japanese bank contracts with a Japanese IT service provider which outsources the service to India, thereby leading to the Japanese bank being subject to Indian law by virtue of business being carried on in India).

Reluctance from foreign, multinational data fiduciaries to do business in India, due to the above concerns, risks hampering innovation and growth for Indian companies and may impede their ability to operate internationally and will ultimately reduce the level of business in India.

Recommendation: Refine the PDPB's extraterritoriality provision to reduce the wide scope of the Bill's applicability. CIPL believes that the law's extraterritorial reach should extend only to those data fiduciaries located outside of India that specifically direct their services to Indian residents and purposefully collect personal data of Indian residents. With respect to issues around conflicts of law, the PDPB might follow a similar approach to the Philippines Data Privacy Act[4] which relieves a processor located in the Philippines from complying with parts of its domestic privacy regime where a foreign controller collected the data in compliance with the laws of its jurisdiction.

Section 3: Definitions

Section 3(2) of the PDPB defines "anonymization" as the "irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the authority". This definition is problematic for several reasons.

[4] Republic Act 10173 — Data Privacy Act of 2012, available at https://www.privacy.gov.ph/data-privacy-act/ at Section 4 — "This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to the immediately succeeding paragraph: Provided, That the requirements of Section 5 are complied with. This Act does not apply to the following: […] g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines".

Firstly, "irreversible" is a very high standard to meet as nothing is completely irreversible. Data should be excluded from the scope of this law when data principals are not identified, having regard to all means reasonably likely to be used, by the data fiduciary or any other person, to identify the data principal. This more realistic standard provides an incentive for organizations to anonymize data using measures appropriate to the risk of identification, which can be assessed through appropriate risk assessment processes for a specific context. When this is coupled with procedural, administrative and legal protections against de-anonymization (e.g. internal accountability measures and a commitment of organizations not to re-identify data; enforceable contractual commitments with third parties not to re-identify data; and legal prohibitions on unauthorized re-identification by any third party), data principals are effectively protected.

Secondly, the standard for anonymization should not be left solely to the data protection authority (DPA). Instead, any standards specified by the DPA should be viewed as guidance that organizations may follow. Organizations should also have the ability and responsibility to identify different or additional anonymization measures that are appropriate for their specific contexts, subject to being able to justify their decisions. This type of shared responsibility for setting reasonable and effective standards would improve the likelihood that personal data are effectively protected and would avoid the legal uncertainty that would result if the standard were left only to the discretion of the DPA.

Recommendation: Revise the definition of anonymization to reflect that it is a process of transforming or converting personal data to a form in which a data principal cannot be identified having regard to all methods reasonably likely to be used by the data fiduciary or any other person to identify the data principal. Incorporate procedural, administrative and legal protections against de-anonymization into the PDPB. Outline a non-exclusive standard for anonymization in the law or in DPA developed guidelines following a public consultation process. Acknowledge that anonymization could also be provided for, or informed by, standards developed by independent bodies, such as the ISO. CIPL also believes that the law should provide for reasonable standards or allowances for re-identification where appropriate. Anonymized data sometimes must be re-identified to provide the benefits derived from the insights gained by analyzing anonymized data to individuals (e.g. a fitness device could provide a certain insight regarding a detected health condition to the user).

Section 13: Processing of personal data necessary for purposes related to employment

The PDPB permits any personal data, except sensitive personal data, to be processed for employment purposes where the consent of the data principal is not appropriate having regard to the employment relationship or would involve a disproportionate effort on the part of the data fiduciary due to the nature of the processing. CIPL believes that sensitive personal data should be included in the scope of this provision as financial data, health data and official identifiers are some forms of data that must be processed in the employment context. For example, to pay salaries, arrange insurance and allocate benefits. CIPL recommends a risk-based approach to privacy protection that requires organizations to subject all of their processing activities to a risk analysis and requires them to establish mitigations and controls appropriate to the risks involved. In the employment context, this means analyzing the risks of using sensitive personal data for employment purposes and mitigating such risks, including through well-defined policies on handling sensitive employee information.

Recommendation: Permit the processing of sensitive personal data for employment purposes.

Section 14: Processing of personal data for other reasonable purposes

The reasonable purposes ground in the PDPB is similar to the concept of "legitimate interest" found in other data protection laws around the world which has proven vital to enabling data fiduciaries and processors to collect and process data while ensuring organizational accountability and respecting data protection rights of individuals.

Currently, the PDPB states that personal data may be processed without obtaining consent if such processing is necessary for such reasonable purposes as may be specified by regulations, after taking into account multiple factors listed in the PDPB, including whether the data fiduciary can reasonably be expected to obtain the consent of the data principal.

CIPL believes that the reasonable purposes ground should not be limited to a rigid list of processing activities as specified by regulations. Organizations should have flexibility to determine when the processing of personal data under reasonable purposes would be most appropriate in line with the specific risk assessment it is required to carry out under the PDPD (i.e. taking into consideration the interests of the data fiduciary, the public interest for the processing, the effect of the processing on rights of the data principal and his or her reasonable expectations).

Furthermore, the reasonable purposes ground should be considered an equal ground with consent and not a residuary ground. Indeed, when implemented properly through the necessary risk assessments and balancing tests, it can provide more effective privacy and data protections than consent. At present, the PDPB lists "whether the data fiduciary can reasonably be expected to obtain the consent of the data principal" as one of the considerations for processing data for reasonable purposes. Consent should not be the default and principal method for processing personal data in India. While consent remains useful for processing data in certain scenarios, there are many contexts and circumstances in the modern information age in which obtaining consent is impractical, impossible, ineffective and simply not meaningful. For example, (1) where there is no direct interaction with individuals, (2) where the data use is common, trivial and imposes no real privacy risk, (3) where large and repeated volumes of data are processed (seeking consent at every instance may not be feasible or may be meaningless as a result of consent fatigue) or (4) where obtaining consent would be counterproductive such as where data is processed to prevent fraud or crime.[5]

Recommendation: Remove the condition that reasonable purposes be specified by regulations and leave that determination to organizations on the basis of the rigorous balancing test outlined in the PDPB and through their consideration of other available grounds for processing. Ensure that the reasonable purposes ground is placed on equal footing with other grounds for processing by removing the requirement to consider whether consent can be reasonably obtained before using this ground. In addition, CIPL recommends that the reasonable purposes ground be renamed "legitimate interest" to facilitate interoperability between different privacy regimes, prevent disruption to business negotiations and commercial data negotiations where parties are not familiar with local legal terminology and to

[5] See "Are Our Privacy Laws Asking Too Much of Consumers and Too Little of Businesses?", CIPL Blog – A Very CIPL Solution: Perspectives on effective and accountable data use, governance, data protection and privacy, 13 December 2019, available at https://www.informationpolicycentre.com/cipl-blog/are-our-privacy-laws-asking-too-much-of-consumers-and-too-little-of-businesses.

ensure that explanations to individuals of why their data was processed and on which basis is universal as they increasingly use and access global services and products.

Section 25: Reporting of personal data breach

Under the current text of the PDPB, the Indian DPA determines whether a data breach should be notified to the data principal, "taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm". CIPL believes that the decision to notify data principals of a breach should be left to the data fiduciary and that the threshold for such notification be more clearly stated as "likely high risk" or "significant harm". This would provide more clarity on the current wording and help avoid over-inclusive notification which could lead to notice fatigue and ultimately diminish the usefulness of such notices to data principals. It would also avoid the additional burden on the DPA to review and determine if a notification to individuals is required in every single data breach. Of course, the DPA should retain the ability to require such notification where necessary and in specific cases.

Moreover, CIPL recommends expanding the provision on data breach notification to provide exceptions to such a notification requirement where the data fiduciary has in place protective measures with respect to the affected data, such as encryption, that make the data unintelligible; or where the data fiduciary has taken measures that reduce any "high risks" so they are no longer likely to materialize; or where the notification would require a disproportionate effort, in which case an alternative way to notify the breach via public communication or similar methods should be permitted.

Finally, with respect to the timing of the notification, the PDPB currently requires the data fiduciary to notify the DPA of a breach as soon as possible and within such period as may be specified by regulations. CIPL cautions against stating any specific timeframe for notification within the law or through the regulations (e.g. 72 hours). Rather, the regulations or the PDPB itself should make clear that notification should occur "without undue delay" after the data fiduciary has awareness and sufficient information about the nature of the breach, including of its likely impact and general significance. The time required for these activities cannot be universally defined in advance and any premature notification may lead to unnecessary and wasteful engagement of the DPA.

Recommendation: Revise the requirement that the DPA should determine whether a data breach should be notified to the data principal and place this responsibility primarily on organizations. Expand the data breach notification provision to include exceptions to notification in line with the recommendations stated above. Clarify in the PDPB or in regulations that the standard for notification should be "without undue delay" after the data fiduciary has awareness and sufficient information about the nature of the breach.[6]

[6] See, generally, US Chamber of Commerce and Hunton Andrews Kurth, LLP, "Seeking Solutions: Aligning Data Breach Notification Rules Across Borders", available at https://www.huntonak.com/en/insights/seeking-solutions-aligning-data-breach-notification-rules-across-borders.html.

Section 26: Classification of data fiduciaries as significant data fiduciaries

The PDPB currently requires the DPA to notify any fiduciary or class of data fiduciary as a significant data fiduciary based on a set of specific factors outlined in the Bill. CIPL foresees many complexities and inefficiencies arising with the inclusion of such a provision in the PDPB.

Firstly, it would impose significant administrative and oversight burdens on the DPA who would be obligated to identify significant data fiduciaries in a process that would have to be constantly repeated and re-assessed in the ever-changing environment of digital and data-driven organizations. The PDPB already outlines an enormous number of tasks that the DPA will be responsible for carrying out and adding such a requirement will likely hamper the effective functioning of the Indian DPA. Secondly, the registration requirement would impose significant administrative burdens and costs on both organizations and the DPA. In addition, the PDPB does not specify which types of data fiduciaries will be required to register – will the registration capture an entire organization or just the particular processing operation that is captured by a factor for "significant data fiduciary"? What if the majority of an organization's processing is not captured? Must such organizations still register? Thirdly, the factors identified as relevant to such classification do not necessarily in and of themselves signify higher risk-levels that would warrant the automatic application of the identified obligations. For example, merely using a new technology may not increase the risk profile of an organization or a processing operation or, by itself, justify a full-blown DPIA or annual audit by an independent data auditor.

Recommendation: Remove the concept of significant data fiduciary from the Bill and apply the specific requirements relevant to such significant data fiduciaries (e.g. conducting DPIAs, maintaining records of processing and appointing a data protection officer) by including the standard of compliance with such provisions in their respective sections.

Section 30: Data protection officer

Currently, a data protection officer appointed under the PDPB must be based in India. CIPL believes that this requirement is excessive. Specifying the geographical location of a DPO would add additional administrative burdens on organizations without any direct corresponding benefits to individuals' privacy and would create barriers and costs to doing business in India. In addition, such a requirement would potentially apply to a large number of organizations with no physical operations in India to appoint DPOs there. Furthermore, the DPO responsibilities and tasks as described in the PDPB can be performed regardless of the physical location of the DPO.

Recommendation: Remove the location requirement for the appointment of a DPO. If India wants to ensure certain organizations established outside of India, but processing Indian personal data, have some kind of representation in India, it might follow the EU General Data Protection Regulation (GDPR) model of requiring a legal representative of the data fiduciary in India.[7]

[7] See Article 4(17) and 27 GDPR.

Section 33: Prohibition of processing of sensitive personal data and critical personal data outside India

The value and importance of global data flows to the Indian economy is undisputed.[8] It is imperative that the PDPB include sensible and realistic rules on cross-border data transfers in order for India to continue to flourish as a global center of innovation and trade for both multinational and domestic India organizations.

While sensitive personal data can be transferred outside of India, the PDPB currently requires that it continue to be stored in India. Such a requirement will not serve the protection of personal data and will severely disrupt the operations of both data fiduciaries and processors in multiple respects. For example, by raising costs to prohibitive levels for foreign small and medium enterprises to enter the Indian market, by imposing the creation of redundant storage systems, by prohibiting use of technologies that rely on the distribution of data (e.g. cloud computing, data analytics and AI), by compromising security of data by preventing its distribution across jurisdictions (e.g. via sharding), etc.

Critical personal data can only be processed in India but may be transferred outside of India in specific limited circumstances. CIPL understands that such a requirement may be motivated around concerns to secure access to data in cross-border investigations of serious crimes. CIPL believes that there are other methods for achieving such access – for instance, via bilateral instruments such as under the US CLOUD Act[9] or under specific trade agreements (see, for example, Article 17.18(2) of the USMCA[10] which does not require financial institutions to store data locally as long as relevant authorities are able to access the information they require). Importantly, critical personal data is not yet defined and the PDPB gives the Indian government broad authority to notify certain categories of data as critical personal data. CIPL recommends, to the extent this concept is retained in the PDPB, the legislature define it narrowly and limit the definition to specific cases related to national security, classified information or national defense.

Recommendation: Remove the local processing and storage requirements for sensitive and critical personal data. Cross-border data flows should be protected, and the appropriate level of privacy protection ensured via an "adequacy" finding of a country, international organization or sector, and via technical and legal measures, including contracts and accountability-based frameworks such as enforceable corporate rules, codes of practice, codes of conduct and certifications, some of which are already included in the PDPB.

---

[8] See "The Data Revolution: Capturing the Digital Trade Opportunity at Home and Abroad", Hinrich Foundation, July 2019, available at https://s3-ap-southeast-1.amazonaws.com/hinrichfoundation-images/wp-content/uploads/2019/10/HF-Digital-Trade-Countries-D4-Red1.pdf, discussing the domestic and export value of digital trade. For example, "[d]igital trade has already created huge positive impact for India's domestic economy, contributing $32.5 billion in 2017. In the right setting, this opportunity could grow by more than 14-fold to reach $480 billion by 2030" and "[d]igital exports represent the largest export sector for India today. The export value of virtual goods and services enabled by the digital economy, such as e-commerce, account for $54.6 billion today, making it India's largest export sector."

[9] Public Law 115-141: Clarifying Lawful Overseas Use of Data (CLOUD) Act, available at https://www.govinfo.gov/content/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm.

[10] United States-Mexico-Canada Agreement, Article 17.18(2), available at https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.

Section 34: Conditions for transfer of sensitive personal data and critical personal data

The PDPB imposes stringent requirements for the transfer of sensitive and critical personal data outside of India. In the case of sensitive personal data, such data may be transferred—once consent is obtained from the data principal—(1) via contract or intra-group scheme, (2) where the Indian government has made a finding of adequacy with respect to the recipient country or organization, or (3) where the Indian DPA has permitted the transfer for any specific purpose.

Critical personal data may only be transferred outside of India where (1) the transfer is to a person or entity engaged in the provision of health or emergency services where such transfer is necessary for prompt action or (2) where the receiving country or organization has obtained adequacy from the Indian government and where the transfer would not affect security and the strategic interest of India.

CIPL believes that contracts, intra-group schemes and adequacy decisions are sensible mechanisms to enable cross-border transfers and consistent with approaches taken in other modern privacy laws such as the GDPR. However, the requirement to obtain an individual's consent alongside such mechanisms is an outlier among data protection laws globally and will seriously impact the ability of organizations to transfer data abroad for legitimate and beneficial purposes.

Indeed, the GDPR only allows for the use of explicit consent as a basis for transfer in cases where a transfer cannot be made pursuant to an adequacy finding or an appropriate safeguard (e.g. binding corporate rules, standard contractual clauses, codes of conduct or certifications) and the individual has been informed of the possible risks of the transfer.

There are a plethora of reasons against creating a consent requirement for cross-border transfers:

- Requiring consent for transfers on top of a contract or intra-group scheme does not necessarily add any additional protection to individuals and obfuscates the fact that an organization has a separate and clear legal obligation to protect the data in line with the contract or intra-group scheme.

- Asking for consent for all cross-border transfers is confusing to individuals and could mislead people to think that there might be something inherently risky or wrong with such transfers. This is the wrong message to send to individuals in a modern global digital economy where such transfers are commonplace, routine and necessary.

- Being asked to consent to every transfer would dramatically increase the number of consent requests and this would burden individuals and have the effect of diluting and undermining the effectiveness of consent in situations where it would be meaningful.

- A new consent requirement for transfers would impose significant burdens on organizations that would have to implement the mechanisms and procedures associated with it and could cause substantial cost and disruption to businesses.

- In some cases, it is impossible to obtain consent at all for a transfer due to an organization's lack of relationship with, and/or contact information of, an individual whose personal data is being

transferred. This is particularly common in outsourcing models and the provision of services related to fighting financial crime, where an organization does not have a direct relationship with the individual in question.

Moreover, in the absence of a definition of critical personal data, many different categories of data could potentially be limited to transfers under extremely narrow exceptions which would indirectly impose a data localization requirement for a whole range of data categories.

CIPL believes that consent is a useful way to legitimize the transfer of data where an appropriate mechanism is not otherwise available. However, combining consent requirements on top of other conditions for transfers will be wholly unworkable in practice.

Recommendation: Reframe the conditions for the transfer of sensitive personal data to permit transfers via contracts, intra-group schemes or adequacy decisions without additionally requiring explicit consent. Reserve explicit consent as a means of transferring data where alternative protections are not available, such as an adequacy finding, contract or intra-group scheme. To the extent the concept is retained in the law, define critical personal data narrowly to avoid unintended categories of data being limited to transfer under extremely narrow exceptions.

Section 37: Power of Central Government to exempt certain data processors

The PDPB permits the central government to exempt certain data processors from the Act that are processing personal data of data principals outside of India, pursuant to any contract entered into with any person/company incorporated outside the territory of India. CIPL welcomes this provision and recommends clarifying that the exemption equally applies to the processing of sensitive personal data. CIPL further recommends that the provision be expanded to expressly exempt global service centers from the application of the Act where such centers are processing the personal data of data principals outside of India and whose personal data is already subject to the privacy laws of their jurisdiction.

Recommendation: Clarify that if the central government exempts a data processor processing personal data of data principals outside of India from the application of the Act, such exemption also applies to the processing of sensitive personal data of such data principals. Expand Section 37 of the PDPB to expressly exempt global service centers from the application of the Act where such centers process the personal data of data principals outside of India.

Section 50: Codes of practice

While CIPL appreciates the inclusion of Codes of Practice within the PDPB, including for purposes of transferring data outside of India, CIPL believes the provision should be broadened to also include privacy seals, marks and certifications. Indeed, in a recent study by CISCO examining the value of privacy certifications in the buying process when selecting a vendor or product, India placed the highest importance on privacy certifications out of the 13 countries surveyed at 95%.[11] These mechanisms would

[11] "From Privacy to Profit: Achieving Positive Returns on Privacy Investments", CISCO Data Privacy Benchmark Study, January 2020, available at https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf at page 12.

not only provide additional important tools for ensuring domestic compliance, organizational accountability and responsible data use in line with the PDPB, but would also facilitate global interoperability between different privacy regimes and serve as additional cross-border transfer mechanisms that ensure the protection of sensitive data when it travels outside of India. With respect to the latter point, by enabling certifications for cross-border transfer purposes, India would ensure protection of the sensitive information at the level prescribed by the PDPB, regardless of where or to whom the data is transferred. Moreover, privacy certifications enabled by and implementing the PDPB could be made interoperable with other global privacy certifications, such as the APEC Cross-border Privacy Rules (CBPR) or GDPR certifications. In addition, having certifications would make it possible for India to join the CBPR system in the future when and if that system is extended to allow direct participation by countries outside of the current APEC member economies. In short, including privacy certifications in the PDPB would provide an additional domestic compliance tool as well as a cross-border transfer tool that would allow data to flow outside of India, including for its economic benefit, without compromising the protection of the personal information being transferred.

Recommendation: Expand the provision on Codes of Practice to include certifications, privacy seals and marks, including for purposes of cross-border data transfers.

Section 91: Act to promote framing of policies for digital economy

The PDPB currently permits the central government, in consultation with the DPA, to direct any data fiduciary or processor to provide any personal data anonymized or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the central government. While CIPL supports accountable data sharing between organizations in both the public and private sectors for social good, CIPL believes that such a provision is inappropriate for inclusion in the PDPB.

Including such a requirement in the law will likely trigger concern among organizations, both domestic and foreign, with respect to the protection of their intellectual property rights and trade secrets. It may also trigger privacy concerns in cases where anonymized data may be re-identified through matching with publicly available data or other obtained datasets. In addition, as this provision applies to data processors as well as data fiduciaries, foreign organizations may be reluctant to utilize Indian data processors as such a requirement will likely breach contractual arrangements between the parties to utilize the data only under the instructions of the data fiduciary and will furthermore put Indian processors at risk of being in non-compliance with the PDPB. Moreover, if the PDPB provisions on extraterritoriality remain in their current form, a foreign company may have no knowledge that the data it is responsible for protecting is being provided to the central government in cases where one of its foreign processors outsources the work or transfers the data to India.

Recommendation: Remove the provision permitting the central government to request any anonymized personal data or other non-personal data from data fiduciaries and processors to enable better targeting of delivery of services or formulation of evidence-based policies by the central government. CIPL believes such a policy should be the subject of a separate discussion relating to accountable data sharing frameworks outside the context of the PDPB and with input from all relevant domestic and international stakeholders given its far reaching application and impact.

Timeline for adoption

The PDPB notes that the Act shall come into force on such date as the central government may appoint via notification in the Official Gazette and that different dates may be appointed for different provisions. It is currently not clear what implementation timeline the central government has in mind. Regardless of whether the final Bill specifies the date the Act will enter into force or whether this is specified via notification by the central government, CIPL recommends providing at least two years for organizations as well as the DPA of India to prepare for the Bill's coming into force. Organizations will have to dedicate sufficient time and resources in preparing for compliance with the law and the DPA will need time to set up its office, assign responsibilities, organize its budget and issue regulatory guidance for organizations.

Drawing on international examples, organizations had two years to implement the EU GDPR in countries that have already had comprehensive data privacy laws in effect for many years with many of the same features as the GDPR and, even then, two years was not sufficient for many organizations. In addition, several international companies which had not reached the requisite level of compliance by 25 May 2018 shut down their service in Europe.[12] Experience has shown that it takes a long time to ensure legacy IT systems and existing uses of data are fully brought into compliance with new rules. Furthermore, policies and procedures may have to be updated, organizational changes may need to occur and, most importantly, organizations will need adequate resources to carry out and implement any significant changes, which typically have to be budgeted several fiscal cycles in advance.

With respect to the DPA, European DPAs saw an intense overhaul of their organizations in the run up to GDPR with many acquiring new staff and increasing their budgets, producing a plethora of regulatory guidance and engaging with industry on hard issues. Brazil's new data protection law, the Lei Geral de Proteção de Dados Pessoais (LGPD) is expected to enter into force in August 2020 and the Brazilian DPA, the ANPD, is still not set up, leaving organizations required to implement that law without a wide range of necessary implementation guidance. Similarly, Thailand's Personal Data Protection Act (PDPA) will enter into effect in May 2020 most likely without an established DPA. Having a data protection framework in place without an established regulator in place in time to develop the necessary rules and guidelines and to oversee the implementation process makes little sense and we advise India to avoid a similar situation by imposing a realistic and sensible implementation timeline for the PDPB following the establishment of a fully operational DPA.

Recommendation: Specify in the PDPB or by notification in the Official Gazette a reasonable, realistic and sensible effective date for the PDPB of at least two years from its passage and/or the establishment of a fully functional DPA to give organizations and the DPA of India adequate time to prepare for the new rules.

[12] See "Startups, Media Companies Block European Users in Wake of New Privacy Laws", Janko Roettgers, 25 May 2018, available at https://variety.com/2018/digital/news/gdrp-sites-blocked-1202822432/.

Conclusion

CIPL is grateful for the opportunity to provide input to the Joint Parliamentary Committee on Bill No. 373 of 2019, the Personal Data Protection Bill. We look forward to future opportunities to comment on and provide input into this process.

If you would like to discuss any of the comments in this paper or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; Sam Grogan, sgrogan@huntonAK.com; Matthew Starr, mstarr@huntonAK.com or Giovanna Carloni, gcarloni@huntonAK.com.