Personal Data Protection Bill 2019
To-dos for companies collecting private data

Most organisations collecting private data of individuals are following the development of data protection legislation in India very keenly. It was anticipated that the Personal Data Protection Bill, 2018 ("**PDPB 2018**") would be enacted into law in early 2019. However, PDPB 2018 underwent certain changes and was tabled before the parliament as the Personal Data Protection Bill, 2019 ("**PDPB 2019**") in the winter session of the parliament on December 11, 2019. The Union Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad thereafter moved motions in both the Lok Sabha and the Rajya Sabha to refer the legislation to a Joint Parliamentary Committee ("**JPC**") for further analysis. The JPC was set up on December 12, 2019 which is headed by BJP MP Meenakshi Lekhi. The JPC is expected make its first report to the Lok Sabha by last week of the Budget Session 2020. In the first meeting of the JPC, which was held on January 16, 2020, the JPC has decided to issue an advertisement and invite all stakeholders to provide their inputs and objections on PDPB 2019 within four weeks.

Set out below, are some of the key provisions of PDPB 2019 which may be applicable to data fiduciaries in India and our suggestions for steps which can be taken by such data fiduciaries to align their operations with the compliance requirements set out in PDPB 2019:

Provisions	Compliance
● Data fiduciaries are required to store all sensitive personal data in India. As per PDPB 2019, sensitive personal data includes data in the nature of financial, health, biometric or genetic data, sexual orientation, religious or political affiliations, caste or tribe, etc. ● Transfer of sensitive personal data is allowed only when explicit consent is given by the data principal for such transfer and if the transfer is made pursuant to a contract or intra group scheme previously approved by the Data protection Authority ("**DPA**"). ● The Government may not approve transfer of sensitive personal data under an intra group scheme unless it provides for effective protection of the rights of data principal as prescribed under PDPB 2019 and liability on the data fiduciary for any harm caused due to non-compliance of the provisions of PDPB 2019.	● Data fiduciaries proposing to transfer customer's sensitive personal data outside the country for processing or storage must include suitable clauses in their documentation with their customers entitling them to do so. These clauses will also require prior approval of the DPA. ● Such data fiduciaries must also identify suitable local data servers or data centres and initiate the process of storing sensitive personal data in India. ● The geographies used by the entities for storage of such customer data must be mentioned in their privacy policy for better transparency.

Provisions	Compliance
• Under PDPB 2018, the data fiduciaries were obligated to store 1 copy of all personal data on local servers or data centres in India. PDPB 2019 has done away with this requirement.	
• Government will notify certain categories of data to be designated as 'critical personal data' which will have to be processed in India and cannot be transferred outside India. PDPB 2019 presently does not provide any indication as to the type of data which might be designated as critical personal data, and this might be notified by the Central Government at a later date.	• Considering that presently there is a lack of clarity on what would constitute critical personal data and the exceptions which might be permitted by the Government, steps in this regard can be taken once the Government has proposed suitable notifications. However, it is safe to assume that any data having impact on national security, health and/or finance of Indian citizens may be designated as critical personal data. •
• As per PDPB 2019, the DPA is empowered to specify appropriate mechanisms for age verification for different data fiduciaries on the basis of the volume of data belonging to children, proportion of data collected which belongs to children and the possibility of harm to children. Parental consent will be required for processing personal data of children. •	• Entities must institute a practice of seeking appropriate documents for verification of the age of the data principals. • If the data principal is found to be below the age of 18 years, then the data fiduciary will have to obtain consent from the parent of such minor in the same manner in which it would otherwise obtain consent from a data principal who is above the age of 18 years.
• PDPB 2019 provides for creation of a "privacy by design policy" by every data fiduciary which must include business practices and technical systems to avoid harm to data principals, obligations of data fiduciary and measures to protect the interest of data principals at every stage of data processing. • Privacy by design policy must be submitted to the DPA for certification.	• Most organisations have already created data privacy policies. These existing policies can be updated to align them with the requirements under PDPB 2019 and include provisions in relation to confirmation, correction and portability of data, RTBF and grievance redressal. The policies should be published on the websites. • These policies can also be maintained in a vernacular/regional language in addition to in English and also all communications with the data principals in India can be made in a vernacular/regional language in addition to in English.
• A 'consent manager' is a data fiduciary registered with the DPA who enables the data principal to	• Smaller data fiduciaries may consider engaging third party consent managers to act

Provisions	Compliance
provide/ withdraw/ manage consents through a transparent platform. ● The consent manager will be required to comply with the conditions specified in the regulations.	as point of contact for data principals allowing data principals to manage their personal data. ● Consent obtained from data principals for collection and processing of personal data needs to be free, informed, specific and withdrawable. The consent forms must be drafted considering these factors.
● The DPA has been vested with wide powers and duties under PDPB 2019 viz. power to call for information, conduct inquiry, search and seizure, take actions, adjudicate complaints, award compensation etc. Data fiduciaries will have to coordinate with the DPA from time to time for various purposes. Further, if any data fiduciary is designated as a 'significant data fiduciary' then such data fiduciary will also have to seek a registration with the DPA.	● It is advisable that data fiduciaries appoint a data protection officer ("**DPO**") to monitor their compliance and liaise with the DPA on their behalf. ● Under PDPB 2019, if the data fiduciary is not based in India then the DPO appointed by such data fiduciary has to be based in India. The DPO must act as a single point of contact for data privacy matters regarding the data fiduciary.
● As per PDPB 2019, every data fiduciary is required to get its processing of personal data audited annually through an independent data auditor. ● The auditor is also empowered to assign a data trust score to the data fiduciary.	● Once PDPB 2019 is enacted and DPA is set up, then DPA shall specify the procedure for the audit. DPA shall also identify and register the data auditors. However, considering the number of data fiduciaries in the country, it seems likely that a suitable infrastructure of data auditors and processes for the audit will take some time to be instituted by the DPA.
● Under PDPB 2019, a data principal has a right to be forgotten ("**RTBF**"). He/she may seek to enforce RTBF on the following grounds: (a) disclosure has served the purpose for which it was made or is no longer necessary; (b) consent has been withdrawn by data principal; or (c) disclosure was made contrary to the provisions of this Act or any other law made by Parliament or any State Legislature.	● The process of RTBF is longer and more cumbersome under PDPB 2019 than under GDPR. However, aggrieved data principals may still seek to enforce this right. Data fiduciaries should consider including suitable provisions in their agreements with data servers and data centres allowing such data fiduciaries to comply with these provisions.
● Offenses under PDPB 2019 are cognizable and non-bailable. Court can take cognizance of offences under PDPB 2019 on a complaint made	● Considering the quantum of proposed punishment and nature of offenses, every

Provisions	Compliance
by the DPA. We assume this insertion has been made from the perspective of providing a strong deterrent against contravention of the provisions of PDPB 2019. ● In case of offense by a company, every person in charge of the company and/or its business will be deemed responsible. Plus, upon proof of involvement of any officer of the company, such officer shall also be deemed guilty. ● If a person is able to prove that the offense was committed without their knowledge or they exercised all due diligence to prevent the offense, such person may not be deemed liable.	data fiduciary should institute robust internal policies to prevent any occurrences breaches. ● The activities of the DPO appointed by data fiduciaries must be adequately monitored by the board of the data fiduciaries to ensure suitable performance. ● Periodic internal/external audits can be undertaken by the data fiduciaries to ascertain compliance. ● Suitable practices must be instituted by data fiduciaries for steps to be taken in case of data breaches, if any. ● Data fiduciaries must institute a grievance redressal mechanism with adequate escalation matrix so that any concerns or complaints of the data principals can be appropriately addressed in a timely manner. ● Under PDPB 2019, a data fiduciary is largely responsible for all actions of 3rd party data processors used by it as well and can be deemed liable for contravention by such data processer. So, it is important that the data fiduciaries also maintain suitable oversight on such 3rd party data processors.

While PDPB 2019 is presently a bill and has not been promulgated into a law, many organisations have already started taking steps to align their operations with the compliance requirements under PDPB 2019, especially considering that the moratorium period of 18 months as provided in PDPB 2018 for enforcement the provisions, inserted to provide adequate time to data fiduciaries to institute processes for complying with all the provisions of the bill, has been done away with in PDPB 2019.

Further as the right to privacy has already been recognized as a fundamental right by the Supreme Court in the matter of *Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India And Ors*. on August 24, 2017, it is always advisable that persons dealing with personal data belonging to others take immediate steps for protection of such data, even if PDPB 2019 has not yet been brought into force.

Presently data privacy related aspects applicable to entities in India are still governed by the provisions of Section 43A of the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 framed thereunder. However, we have observed that many data fiduciaries to whom the provisions of EU General Data

Protection Regulations ("**GDPR**") are applicable, have already instituted practices for data protection in compliance with GDPR.

Disclaimer: *This article is meant for informational purpose only and does not purport to be advice or opinion, legal or otherwise, whatsoever. Pioneer Legal does not intend to advertise its services through this article.*