The Personal Data Protection Bill, 2019

The Personal Data Protection Bill, 2019 ("**PDP Bill**"), which was presented before the lower house of the Indian Parliament on December 11, 2019, seeks to provide for the protection of personal data of individuals and establish a Data Protection Authority ("**DPA**"). The PDP Bill has been referred to a joint select committee of both the houses of the Indian Parliament, which is expected to submit its report in early 2020. Accordingly, there may be changes to the PDP Bill based on the recommendations of the joint select committee. Once enacted, the PDP Bill will replace Section 43 of the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and prevail over any other inconsistent laws in this regard (e.g., any sector-specific laws).

The PDP Bill applies to the processing of personal data by:

A	the Government	**B**	companies incorporated in India	**C**	foreign companies dealing with personal data of individuals in India

It covers the following categories of information:

1. **"personal data":** any data about or relating to a natural person who is directly or indirectly identifiable having regard to any attributes or characteristics of such person (online or offline) and includes any inference drawn from such data for the purposes of profiling

2. **"sensitive personal data":** a subset of personal data which may reveal, relate to or constitute financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation. Additionally, the Central Government in consultation with the DPA and the sectoral regulators, notify other categories of personal data as sensitive personal data; and

3 **"critical personal data":** a subset of personal data and will include such categories of personal data as may be notified by the Central Government

The PDP Bill does not apply to the processing of anonymized data, i.e., personal data that has been irreversibly transformed or converted to a form in which a data principal cannot be identified in a manner that meets the standards prescribed by the DPA.

NOTICE, CONSENT AND PURPOSE

The PDP Bill sets out certain rights of a "data principal", i.e., the individual whose personal data is collected, including to correct incomplete or inaccurate personal data, erase personal data that is no longer required for the consented purpose and the right to be forgotten.

A "data fiduciary", i.e., an entity or individual who decides the means and purpose of processing personal data, is permitted to collect personal data subject to the consent of data principals and such personal data can be processed only for the purpose consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect the use of such personal data. Further, explicit consent will be required for collecting sensitive personal data.

The data principal may give or withdraw her consent to the data fiduciary through a consent manager (an entity registered with the DPA which a data principal may use to gain, withdraw, review and manage her consent). Regulations in relation to the registration and other obligations of a consent manager are proposed to be issued by the DPA.

The consent requirement has been dispensed with in certain specified cases, for e.g., the performance of any lawful function of the State, compliance with any order/judgment of any court, a medical emergency, disaster or breakdown of public order and an employment-related purpose. Additional grounds for exemption from the consent requirement are under the category of "reasonable purpose" (which includes mergers and acquisitions, recovery of debt, operation of search engines and whistle blowers) and may be notified by the DPA.

A data fiduciary is required to give notice to the data principal at the time of collection of personal data or as soon as reasonably practicable where the data is not collected from the data principal with certain prescribed details, including the purpose of collection; identity and contact details of the data fiduciary and data protection officer, if applicable; procedure for withdrawal of consent; basis for such processing and consequences of failure to provide personal data; source of collection (if not collected from the data principal); persons with whom the personal data may be shared; information regarding any cross-border transfer of personal data; period for which the personal data will be retained and procedure for grievance redressal.

The PDP Bill clarifies that provision of any goods or services to the data principal cannot be made conditional on the consent of such data principal to the processing of any personal data that is not necessary for such purpose.

DATA LOCALIZATION

Sensitive personal data and critical personal data are required to be stored in India.

Sensitive personal data

Sensitive personal data is permitted to be transferred outside India only in certain cases (e.g., where the transfer is made pursuant to a contract or scheme approved by the DPA or the Central Government has allowed the transfer to a country or entity or class of entity subject to satisfaction of certain conditions or where the DPA has allowed such transfer for a specific purpose), provided that such data continues to be stored in India and explicit consent has been obtained in this regard from the data principal.

Critical personal data

The processing of critical personal data outside India is prohibited under the PDP Bill. However, the transfer of such critical personal data is permitted to a person or entity engaged in provision of health services or emergency services in specified circumstances or to any country or entity or class of entity approved by the Central Government subject to the satisfaction of certain conditions and where such transfer in the opinion of the Central Government does not prejudicially affect the security and strategic interest of India.

OTHER OBLIGATIONS OF DATA FIDUCIARIES

In addition to the obligations discussed above, the PDP Bill imposes several obligations on data fiduciaries. Data fiduciaries will be required to put in place necessary safeguards for complete, purposeful and accurate processing of the personal data, implement a privacy by design policy that is certified by the DPA and an effective mechanism to redress grievances of data principals, notify instances of breach to the DPA and undertake periodic review to ensure that personal data is not retained beyond the period necessary to satisfy the purpose for which it was processed unless there is explicit consent. The PDP Bill prescribes additional compliance responsibilities on the data fiduciaries which process personal and sensitive data of children.

Data fiduciaries may be designated as significant data fiduciaries ("**SDF**") on the basis of considerations such as volume of personal data processed, sensitivity of the personal data processed, turnover of the data fiduciary or any other considerations as may be specified by the DPA. The Central Government may also notify certain types of social media intermediaries (other than intermediaries that primarily enable commerce or business oriented transactions, provide access to internet or are search engines, e-mail services, storage services or encyclopedias) as SDFs. SDFs will be required to undertake additional

compliances in the manner prescribed by the DPA, including conducting a data protection impact assessment, arranging an audit of its policies by an independent data auditor and appointing a data protection officer.

EXEMPTIONS

The PDP Bill provides exemptions from certain provisions in specified cases, for example, provisions relating to consent requirement, data localization and certain other obligations of data fiduciaries where disclosure of personal data is necessary for the prevention, detection, investigation and prosecution of any offence, enforcing any legal right/claim or by a court or tribunal or for any personal or domestic purpose by a natural person or for any journalistic purpose.

The PDP Bill also contemplates the creation of a 'sandbox' to encourage innovation in artificial intelligence, machine-learning or any other emerging technology in public interest. Details regarding registration by eligible entities and the relaxations proposed to be extended to such entities under the sandbox will be issued by the DPA.

Additionally, the PDP Bill states that the Central Government has the power to exempt any agency of the Government from complying with the provisions of the PDP Bill in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States and public order. This discretionary power of the Central Government does not appear to be subject to any limitations.

PENALTIES

Similar to the European Union's General Data Protection Regulation, the PDP Bill prescribes penalties which can be imposed on a data fiduciary. These penalties may extend to the higher of a maximum of Rs.150 million or 4% of such data fiduciary's total worldwide turnover for the preceding financial year. The PDP Bill also prescribes criminal sanctions where a person re-identifies and processes personal data without the consent of data fiduciary or a data processor which has de-identified such personal data. An aggrieved data principal is also entitled to recover compensation from the data fiduciary or the data processor on making a complaint to the relevant adjudicating officer in event of a violation of his rights under the PDP Bill.

CONCLUSION

The PDP Bill is welcome step forward to address the needs of an evolving data protection regime of India. However, several aspects of data protection (such as categorization of personal data as sensitive personal data and critical personal data, details on anonymized data, conditions from exemption from certain provisions of the PDP Bill, categories of SDFs, conditions for registration as a consent manager and processing of personal data and sensitive personal data of children), which will be key to an effective and successful implementation of the new regime, have been delegated to the DPA and/or the Central Government. Accordingly, the real impact of the PDP Bill will be visible once the relevant

rules and regulations are in place.

The PDP Bill does not provide for any transitional provisions and timelines for implementation. Currently, the PDP Bill contemplates that the provisions will come into force the day they are notified in the official gazette of India (which will occur after the approval of the Indian Parliament and the President of India). We are hopeful that the PDP Bill, in its final form, provides companies sufficient time to conform their business practices to ensure compliance with the PDP Bill. Nevertheless, corporates in India that would get categorized as a data fiduciary under the PDP Bill should review their existing data protection framework.

*This insight has been authored by **Radhika Iyer** (Partner), **Lakshmi Pradeep** (Associate) and **Anshul Chopra** (Associate). They can be reached on riyer@snrlaw.in, lpradeep@snrlaw.in and achopra@snrlaw.in for any questions.*