Bill Analysis: Personal Data Protection Bill, 2019

In 2018, Justice B.N. Srikrishna Committee submitted its report to the Ministry of Electronics and Information Technology for a data protection framework in India. On the basis of this report, the Personal Data Protection Bill, 2018 was drafted. However, it was never tabled before the Parliament and an amended version of this Bill, the Personal Data Protection Bill, 2019 (**"PDP Bill"**) was introduced in the Lok Sabha in December 2019. The Bill is presently referred to a Joint Parliamentary Committee. An attempt is made here to analysis certain highlights of the PDP Bill.

Important Terms

- Valid **"consent"** has been defined as consent which is specific, freely given, informed, clear, and capable of being withdrawn. It is important ascertain whether consent obtained is valid or not, because under the PDP Bill, personal data cannot be processed unless the "data principal consents" to such processing. However, this is subject to certain exceptions.
- A "Data Fiduciary" has been defined as "any person who determines the purposes and means of processing of personal data". In simple words, these entities control how personal data is collected and how it will be utilized. A category of data fiduciaries is also created under the PDP Bill as "significant data fiduciaries". A "significant data fiduciary" has additional obligations under the PDP Bill, as will be discussed below.
- Further, a "Data Processor" has been defined as "any person who processes personal data on behalf of a data fiduciary". A data fiduciary may itself be a data processor if it "processes" data. However, data fiduciaries outsource many processing activities such as "profiling" to other entities. These entities are referred here as "data processors". Definition of "processing" and "profiling" is also present in the PDP Bill.
- "Data Principal" has been defined as the "the natural person to whom the personal data relates". "Personal Data" has been defined as data which directly or indirectly leads to identification of a natural person. Certain categories of personal data have also been defined, namely "anonymized data" and "sensitive personal data". "Sensitive personal data" has been defined to include, inter alia, "biometric data", "financial data", "genetic data", "health data". There are additional obligations on data fiduciaries regarding processing of sensitive personal data.

- "Processing" has been defined to include, inter alia, collection, recording, structuring, storage and transferring of personal data.

Rights of the Data Principal

The PDP Bill gives the "Data Principal" certain rights over its personal data. These rights include:

- Right to withdraw consent for processing of data
- Right to confirmation and access to processing of personal data
- Right to correction and erasure of personal data
- Right to data portability in a "structured, commonly used and machine-readable format"
- Right to be forgotten by restricting or preventing the disclosure of personal data
- Right to file a complaint with the Data Protection Authority (**"DPA**")

Obligations imposed on the "Data Fiduciaries" as well as on the "Data Processors"

The PDP Bill lays down certain obligations applicable equally on the "data fiduciaries" as well as on the "data processors". These obligations include:

- Processing personal data only for "specific, clear and lawful" purposes.
- Processing personal data "in a fair and reasonable manner" and ensuring "privacy of the data principal".
- Processing personal data only for purposes which are consented upon and reasonably expected by the data principal.
- Collecting personal data only to extent necessary for purposes of processing.
- Implementing necessary security safeguards by running risk assessments and reviewing such safeguards periodically.

Obligations imposed only on the "Data Fiduciaries"

The PDP Bill lays down certain obligations specifically on "data fiduciaries". These obligations include:

- Ensuring "quality" of personal data. To ensure "quality" of personal data, it must be complete, accurate, updated, and not misleading.
- Not retaining personal data "beyond the period necessary to satisfy the purposes" of processing.
- Preparing a "privacy by design" policy which, inter alia, talks about protection of privacy.
- Ensuring "transparency" in processing.

- Giving notice to the data principal of information regarding, inter alia, purposes of processing, nature and categories of personal data collected and third parties to whom personal data would be shared.
- Reporting of "data breach" to the DPA "where such breach is likely to cause harm".

Obligations of Significant Data Fiduciary

The "significant data fiduciaries" would be notified by the DPA by taking into account, inter alia, the volume and sensitivity of personal data processed by such entities. Other than the usual obligations that are imposed on data fiduciaries, the significant data fiduciaries have additional obligations under the PDP Bill. These obligations include:

- Conducting "Data Protection Impact Assessment", which will, inter alia, assess the "potential harm that may be caused to the data principals".
- Maintaining accurate and updated records of, inter alia, collection and transfers of personal data, periodic review of security safeguards, and data protection impact assessments.
- Getting audits of policies and conduct of processing, by independent auditors.
- Appointing "Data Protection Officer" for, inter alia, providing advice to such significant data fiduciary.
- If appointing a data processor, then it must be made ONLY in pursuance of a contract between such processor and the significant data fiduciary.

The "Data Protection Authority" of India

The PDP Bill envisages establishment of a "Data Protection Authority" of India. The DPA has four primary functions, namely, enforcement of the PDP Bill, setting standards, research, and adjudication. The DPA will also issue "Codes of Practice" to facilitate compliance of the PDP Bill. Moreover, the DPA has the power to issue directions to data fiduciaries/processors, call for information from them and to also conduct inquiries on its own motion or on the basis of a complaint. Violation of the provisions of the PDP Bill attracts as high as 15 Crore rupees or 4% of entity's total worldwide turnover of the preceding financial year, whichever is higher. Moreover, the data principal also has a right to seek compensation from the data fiduciary/processor by filing an application to the DPA's adjudicating officer.

Restrictions on Cross-Border Transfer of Sensitive Personal Data

The PDP Bill allows transfer of sensitive personal data outside India with "explicit consent" of the data principal subject to certain other conditions but makes it mandatory to keep a copy of such data in India.

Moreover, the Central Government would notify certain categories of sensitive personal data as "critical personal data" which would be processed ONLY in India.

Concluding Remarks

The PDP Bill seeks to regulate the digital economy which remains largely unregulated in India. This article sought to explain, in the simplest manner, what obligations the PDP Bill seeks to impose to convert the existing "opt out" privacy policies into "opt in" policies. This takes away the existing bargaining power from the data fiduciaries to some extent. Establishment of DPA as India's "privacy watchdog" is also a much needed move, as the present CERT-In remains more of a certifying authority than a supervisory authority. While it cannot be said that the PDP Bill is an exact copy of the EU's GDPR, it also cannot be said that it's a complete novelty. It borrows a lot from the GDPR, but makes necessary changes which suit the need of the Indian digital economy. The finest example of this is the case of "significant data fiduciaries". By adding separate obligations on significant data fiduciaries, the PDP Bill ensures distribution of obligations in an equitable manner. This is not the case in the GDPR. For example, a small data fiduciary in India, like an MSME, will not have to conduct data protection impact assessments. This is not the case in GDPR. In GDPR, every data fiduciary has to conduct data protection impact assessments. If this was the situation in India, this would have broken the backs of MSMEs by adding an additional financial burden on them. We will find many such examples throughout the scheme of the PDP Bill. In conclusion, the PDP Bill tries to ensure the privacy of personal data of data principals but at the same time keeps in mind the interests of the digital economy.