Obligations on Businesses vis-à-vis the Personal Data Protection Bill, 2019

DMD® ADVOCATES

A digital economy has immense transformative potential for a country like India. It can significantly improve lives of Indians, given its tremendous contribution to sectors that affect masses such as, healthcare, research and development, emergency services, and transportation, to name a few. However, a booming digital economy also brings about unique challenges and potential for discrimination, exclusion and harm. The admission by Facebook that data of 87 million users (including half a million Indians) was shared with a third-party Cambridge Analytica, which extracted personal data of Facebook users who had downloaded Facebook application as well as personal data of their friends, is demonstrative of one such harm. Unfortunately, the Facebook incident was neither isolated nor exceptional. Currently, the law in India and many other nations across the globe provide limited protection to personal data of individuals.

The inadequacy in the personal data protection regime was first recognized by the European Union ("EU"). Taking a lead, the EU adopted General Data Protection Regulation ("GDPR") on 14 April 2016. A legal framework that requires businesses to protect the personal data and privacy of individuals in the EU and the European Economic Area ("EEA") for transactions that occur within the EU and the EEA. The GDPR was adopted on 14 April 2016 and came into force on 25 May 2018.

In India, the Supreme Court on 24 August 2017, delivered a landmark judgement in Justice K. S. Puttaswamy (Retd.) v. Union of India (WP (Civil) no. 494 of 2012) recognizing the right to privacy as a fundamental right emerging primarily under Article 21 of the Constitution. The Supreme Court also emphasized the need for a data protection framework in India.

On 27 July 2018, a committee led by former Supreme Court Justice B.N. Srikrishna submitted a draft Personal Data Protection Bill, 2018 and a report titled "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" to the government. The Ministry of Electronics and Information Technology ("MeitY") invited stakeholders' comments and conducted consultations on the Personal Data Protection Bill, 2018.

After several rounds of consultation with various stakeholders, MeitY released a revised bill, the Personal Data Protection Bill 2019 ("PDP Bill"). The PDP Bill was introduced in Lok Sabha on 11 December 2019. The Lok Sabha referred the PDP Bill to a Standing Committee, which is expected to submit its report in the last week of the Budget Session, 2020 (expected on 30 March 2020).

Applicability and obligations on companies

The PDP Bill is applicable to personal data which is collected, disclosed, shared or processed in India by data fiduciaries. A 'data fiduciary' is an entity, including the State, a company, a juristic entity, or any individual, that determines the purpose and means of processing of the personal data.

The PDP Bill imposes certain obligations on data fiduciaries as set forth below.

Fair and reasonable processing: Data fiduciaries processing the personal data have a duty to process the personal data of an individual in a fair and reasonable manner respecting the privacy of the individual.

Purpose Limitation: Data fiduciaries are obligated to ensure that the personal data processed by them is only for purposes that are clear, specific and lawful.
Further, the data fiduciaries are obligated to ensure that the personal data is processed only for purposes specified, or for such incidental purposes that an individual, whose data is collected, would reasonably expect the personal data to be used for.

Collection Limitation: Data fiduciaries are required to collect only such personal data which is necessary for the purpose of processing.

Personal Data

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 the natural person. Also, includes any inference drawn from such data for purpose of profiling.

Data Principal

Defined as a natural person to whom the personal data relates.

Obligations on Businesses vis-à-vis the Personal Data Protection Bill, 2019

DMD® ADVOCATES

Lawful Processing: Personal data and sensitive personal data to be processed only on the basis of grounds of processing, specified separately for each in the PDP Bill.

Requirement of notice for collection and processing of personal data: The data fiduciaries are required to provide a notice to individuals at the time of collection of the personal data. If the data is not collected directly from the individual, then the notice must be provided to such individual as soon as is reasonably practicable. However, the notice need not be given if such notice substantially prejudices the purpose of processing of personal data and consent was not required for such processing.

Processing

'Processing' in relation to personal data, means an operation or set of operations performed on the personal data. It includes operations such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

The notice should be clear, concise and easily comprehensible to a reasonable person and must contain the following information:

- Purposes for which the personal data is to be processed and categories of personal data being collected;
- Identity and contact details of the data fiduciary and the contact details of the data protection officer, if applicable;
- Right of the individual to withdraw his/her consent, if the personal data is intended to be processed on the basis of consent and procedure for such withdrawal;
- Basis for processing the personal data and consequences of the failure to provide the personal data;
- Source of collection of personal data, if the personal data is not collected from the individual;
- Individuals or entities including other data fiduciaries or data processors, with whom personal data may be shared;
- Information regarding any cross-border transfer of the personal data;
- Period for which the personal data will be retained and where such period is not known, the criteria for determining such period;
- Existence of and procedure for the exercise of rights of data principals;
- Procedure for grievance redressal;
- Existence of a right to file complaints to the data protection authority;
- Any rating in the form of a data trust score that may be assigned to the data fiduciary; and
- Any other information which may be specified by the data protection authority.

Sensitive Personal Data

Certain personal data has been classified as 'sensitive personal data'.

Sensitive personal data includes personal data that reveals, is related to, or constitutes 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 and any other category of data that may be notified by the government in consultation with the data protection authority and concerned sector regulator.

Data Quality: Data fiduciaries are required to take reasonable steps to ensure that personal data processed is complete, accurate, not misleading and updated, having regard to the purposes for which it is processed.

Data Storage Limitation: The data fiduciaries are required to retain personal data for reasonably necessary time to satisfy the purpose for which it is processed. However, personal data may be retained for a longer period of time if such retention is explicitly mandated, or necessary to comply with any obligation, under a law.

Further, the data fiduciary is required to undertake periodic review in order to determine whether it is necessary to retain the personal data in its possession. If on review, it is determined that it is not necessary for personal data to be retained, then such personal data must be deleted.

Accountability: Data fiduciaries are responsible for complying with all obligations set out in the PDP

Bill with respect to any processing undertaken by it or on its behalf. Further, they must be able to demonstrate that any processing undertaken by them or on their behalf is in accordance with the provisions of the law.

Besides the above obligations, the PDP Bill mandates certain transparency and accountability measures that data fiduciaries are required to undertake. Such transparency and accountability measures include:

- Preparing a privacy by design policy;
- Undertaking necessary steps to maintain transparency in processing personal data;
- Making available information such as, but not limited to, (a) categories of personal data generally collected and the manner of such collection; (b) the purposes for which personal data is generally processed; (c) any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm; (d) the existence of and the procedure for exercise of rights of data principal and any related contact details for the same; (e) the right of data principal to file complaint against the data fiduciary to the data protection authority; (f) any rating in the form of a data trust score that may be accorded to the data fiduciary; and (g) information regarding any cross-border transfers of personal data that the data fiduciary generally carries out.
- Implementing necessary security safeguards such as, but not limited to, use of methods such as de-identification and encryption; steps necessary to protect the integrity of personal data; and steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.
- Undertaking a review of its security safeguards periodically and taking appropriate measures accordingly.
- Reporting personal data breach in the manner specified in the PDP Bill.

Data Localisation and Cross Border Transfer of Data

Transfer of 'sensitive personal data' outside of India is permitted under the PDP Bill subject to certain conditions, however, it can be stored only in India. Sensitive personal data may be transferred outside India if explicit consent is received from the data principal and one of the following additional grounds are also fulfilled:

(a) the transfer is made pursuant to a con tract or intra-group scheme approved by the data protection authority; or
(b) the government has allowed the transfer to a country or, such entity or class of entity in a country or, an international organization on the basis of its finding of adequate level of protection and that such transfer does not affect the enforcement of any other relevant law; or
(c) the data protection authority has allowed transfer of sensitive personal data or class of sensitive personal data necessary for a specific purpose.

'Critical personal data' has not been notified as yet and no guideline has been provided as to what kind of data may be considered as critical personal data. Further, critical personal data may be processed only in India.
Critical personal data may be transferred outside India:

(a) to a person or entity engaged in the provision of health services or emergency services where such transfer is necessary for prompt action; or
(b) if the government has allowed the transfer to a country or, such entity or class of entity in a country or, an international organisation on the basis of its finding of adequate level of protection and such transfer does not prejudicially affect the security and strategic interest of India.

Penalties and Compensation

The PDP Bill imposes stringent penalties and provides compensation to data principals in case data fiduciaries are in contravention of its provisions. Such stringent penalties and compensation are with a view to ensure compliance by data fiduciaries.

Conclusion

While the PDP Bill is a step in the right direction, the implementation looms large as a challenge for the industry as well as the government. On the one hand, the industry awaits with bated breath the release of the final bill and gears up for the significant effort and costs that would entail, on the other, the government has to consider and build the framework to implement the law. Given the scope and powers of the data protection authority, government will have to dedicate substantial time and resources to ensure that law on paper turns into ground reality without any unintended consequences. It is especially important given the present state of the Indian economy and issues grappling it, potentially resulting from shoddy implementation of bold steps and legal and policy changes that the government introduced in recent years.

For any further questions or advise on data privacy law in India, please feel free to contact our data privacy expert:

RASHI DHIR

Email: rashi.dhir@dumeds.com