BUSINESS LAW
CHAMBER

DATA PROTECTION LAWS IN INDIA

Brief : In the awake of Facebook admitting in early 2018 that it shared information of up to 87 million users worldwide with Cambridge Analytica, various countries have been updating their data protection laws for adequate protection of personal data against such scandals. The EU has in place GDPR and various countries have been amending their data protection laws in line of GDPR. In India, the current data protection laws have proven to be insufficient and inadequate to the existing business scenarios. However, the Government of India has proposed the Personal Data Protection Bill, 2018 which is yet to be introduced in the Parliament. This new bill is more onerous and provides stronger provisions to users seeking deletion of their personal information.

1. CURRENT DATA PRIVACY LAW IN INDIA

Primarily, data protection is granted under the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Laws"). In addition to this, sectoral regulators for telecommunication companies, banking companies, medical companies and insurance companies have prescribed regulations to prevent unauthorized disclosures. Although, these Laws protect 'personal information' and 'sensitive personal data or information' ("Information"), however, neither data principles (i.e. the natural persons to whom that data belongs to) have any right nor are there any guidelines on the processing and usage of data. The data protection in India is available against data that is collected by entities located in India. With that said, the Laws provide the following basic protection:

(i)Entities seeking such Information must draft and publish on their website a privacy policy containing the Information that is being collected and purpose of its use.
(ii)Entities must obtain consent from the users before they acquire user's Information.
(iii)Entities must establish reasonable security measures for protection and confidentiality of the Information collected.
(iv)Information can be retained up to the duration of its purpose being fulfilled. The purpose of collecting the data must be well-defined .

Further, the law provides certain entity oriented compliances/reporting, such as Cert-In rules wherein entities storing or processing Information must report to the authority in case of any breach.However, even such measures seem inadequate. Recently, it has been reported that there were security and data breach on WhatsApp that affected 1400 WhatsApp users worldwide and more than 100 Indian users.

In an article by Economic Times on 2nd November 2019, it had been observed that although it appears that WhatsApp has complied with its reporting obligations under the Cert-In rules, it is unclear whether the reporting was adequate and prompt.

These incidents evidence the adequacy of both data protection and data reporting laws of India.

2. EU'S GDPR

Unlike the Indian data protection Laws which are only applicable on entities located in India, the General Data Protection Regulation, 2018 ("GDPR") applies to any entity, whether situated in EU or anyplace else, processing personal information of EU citizens. GDPR bestows certain rights over the EU citizens, i.e. right to be informed, right of access, right of rectification, right to erasure, right to restrict processing, right to data portability, right to object and right not to be subject to automated individual decision-making, including profiling, where the decision will have legal or other significant effects. These rights can be enforced against organisations that process personal data. The law rightly gives a broad definition of 'personal data' as "any information relating to an identified or identifiable natural person. This broad definition does not give any leeway for entities processing personal data and thus, provides greater protection to citizens. Further, GDPR provides that entities cannot process personal data unless consent has been obtained by the respective citizen. Article 5 of the GDPR lays down certain principles for processing of personal data. These are: (i) lawfulness, fairness and transparency, (ii) collecting and processing for legitimate purposes, (iii) collecting only the required data, (iv) processing of data must be accurate, (v) cannot store personal data for indefinite time, (vi) providing adequate security to personal data, and (vii) controller of personal data must be accountable.v

3. PERSONAL DATA PROTECTION BILL, 2018

The Union cabinet approved the bill on 04th December 2018 for introduction in the parliament. The bill is in line with EU's GDPR and aims to provide better protection than the present scattered provisions. It defines sensitive personal data to include passwords, financial data, biometric and genetic data, caste, religious or political beliefs. Further, the bill states any personal data that is collected must be processed only for the purpose it was collected for in the first place. Processing is allowed if the individual gives consent, or in a medical emergency, or by the State for providing benefits. However, the Bill allows exemptions for purposes such as (i) national security (pursuant to a law), (ii) prevention, detection, investigation and prosecution of contraventions to a law, (iii) legal proceedings, (iv) personal or domestic purposes, and (v) journalistic purposes.

Similar to GDPR, the bill also introduces rights of data principle (natural person to whom the personal data relates to) which are similar to the rights under GDPR. These rights include: (i) the right to obtain a summary of their personal data held with the data fiduciary, (ii) the right to seek correction of inaccurate, incomplete, or outdated personal data, (iii) the right to have personal data transferred to any other data fiduciary in certain circumstances, and (iv) the right 'to be forgotten', which allows the data principal to restrict or prevent continuing disclosure of their personal data.

The Bill further lays down certain obligations on the data fiduciary (entity which determines the purpose and means of processing personal data) who is processing personal data. These include: (i) processing personal data in a fair and reasonable manner, (ii) notifying the data principal of the nature and purposes of data collection, and their rights, among others, and (iii) collecting only as much data as is needed for a specified purpose, and storing it no longer than necessary. Personal data (except sensitive personal data which is 'critical') may be transferred outside India under certain circumstances. These include cases where (i) the central government prescribes that transfers to a particular country are permissible, or (ii) the DPA approves the transfer in a situation of necessity.