Report Summary

A Free and Fair Digital Economy

- The Committee of Experts on a Data Protection Framework for India (Chair: Justice B. N. Srikrishna) submitted its report and draft Bill to the Ministry of Electronics and Information Technology on July 27, 2018. The Committee was constituted in August, 2017 to examine issues related to data protection, recommend methods to address them, and draft a data protection Bill.
- **Fiduciary relationship:** The Committee observed that the regulatory framework has to balance the interests of the individual with regard to his personal data and the interests of the entity such as a service provider who has access to this data. It noted that the relationship between the individual and the service provider must be viewed as a fiduciary relationship. This is due to the dependence of the individual on the service provider to obtain a service. Therefore, the service provider processing the data is under an obligation to deal fairly with the individual's personal data, and use it for the authorised purposes only.
- **Obligations of fiduciaries:** To prevent abuse of power by service providers, the law should establish their basic obligations, including: (i) the obligation to process data fairly and reasonably, and (ii) the obligation to give notice to the individual at the time of collecting data to various points in the interim.
- **Definition of personal data:** The Committee noted that it is important to define what constitutes personal information. It defined personal data to include data from which an individual may be identified or identifiable, either directly or indirectly. The Committee sought to distinguish personal data protection from the protection of sensitive personal data, since its processing could result in greater harm to the individual. Sensitive data is related to intimate matters where there is a higher expectation of privacy (e.g., caste, religion, and sexual orientation of the individual).
- **Consent-based processing:** The Committee noted that consent must be treated as a pre-condition for processing personal data. Such consent should be informed or meaningful. Further, for certain vulnerable groups, such as children, and for sensitive personal data, a data protection law must sufficiently protect their interests, while considering their vulnerability, and exposure to risks online. Further, sensitive personal information should require explicit consent of the individual.
- **Non-consensual processing:** The Committee noted that it is not possible to obtain consent of the individual in all circumstances. Therefore, separate grounds may be established for processing data without consent. The Committee identified four bases for non-consensual processing: (i) where processing is relevant for the state to discharge its welfare functions, (ii) to comply with the law or with court orders in India, (iii) when necessitated by the requirement to act promptly (to save a life, for instance), and (iv) in employment contracts, in limited situations (such, as where giving the consent requires an unreasonable effort for the employer).
- **Participation rights:** The rights of the individual are based on the principles of autonomy, self-determination, transparency and accountability to give individuals control over their data. The Committee categorised these rights in three categories: (i) the right to access, confirmation and correction of data, (ii) the right to object to data processing, automated decision-making, direct marketing and the right to data portability, and (iii) the right to be forgotten.
- **Enforcement models:** The Committee also recommended setting up a regulator to enforce the regulatory framework. The Authority will have the power to inquire into any violations of the data protection regime, and can take action against any data fiduciary responsible for the same. The Authority may also categorise certain fiduciaries as significant data fiduciaries based on their ability to cause greater harm to individuals. Such fiduciaries will be required to undertake additional obligations.
- **Amendments to Other Laws:** The Committee noted that various allied laws are relevant in the context of data protection because they either require or authorise the processing of personal data. These laws include the Information Technology Act, 2000, and the Census Act, 1948. It stated that the Bill provides minimum data protection standards for all data processing in the country. In the event of inconsistency, the standards set in the data privacy law will apply to the processing of data. The Committee also recommended amendments to the Aadhaar Act, 2016 to bolster its data protection framework.

Roshni Sinha
roshni@prsindia.org

August 1, 2018

Bill Summary

The Draft Personal Data Protection Bill, 2018

- **Rights of the individual:** The Bill sets out certain rights of the individual. These include: (i) right to obtain confirmation from the fiduciary on whether its personal data has been processed, (ii) right to seek correction of inaccurate, incomplete, or out-of-date personal data, and (iii) right to have personal data transferred to any other data fiduciary in certain circumstances.
- **Obligations of the data fiduciary:** The Bill sets out obligations of the entity who has access to the personal data (data fiduciary). These include: (i) implementation of policies with regard to processing of data, (ii) maintaining transparency with regard to its practices on processing data, (iii) implementing security safeguards (such, as encryption of data), and (iv) instituting grievance redressal mechanisms to address complaints of individuals.
- **Data Protection Authority:** The Bill provides for the establishment of a Data Protection Authority. The Authority is empowered to: (i) take steps to protect interests of individuals, (ii) prevent misuse of personal data, and (iii) ensure compliance with the Bill. It will consist of a chairperson and six members, with knowledge of at least 10 years in the field of data protection and information technology. Orders of the Authority can be appealed to an Appellate Tribunal established by the central government and appeals from the Tribunal will go to the Supreme Court.
- **Grounds for processing personal data:** The Bill allows processing of data by fiduciaries if consent is provided. However, in certain circumstances, processing of data may be permitted without consent of the individual. These grounds include: (ii) if necessary for any function of Parliament or state legislature, or if required by the state for providing benefits to the individual, (iii) if required under law or for the compliance of any court judgement, (iv) to respond to a medical emergency, threat to public health or breakdown of public order, or, (v) for reasonable purposes specified by the Authority, related to activities such as fraud detection, debt recovery, and whistle blowing.
- **Grounds for processing sensitive personal data:** Processing of sensitive personal data is allowed on certain grounds, including: (i) based on explicit consent of the individual, (ii) if necessary for any function of Parliament or state legislature, or, if required by the state for providing benefits to the individual, or (iii) if required under law or for the compliance of any court judgement.
- Sensitive personal data includes passwords, financial data, biometric data, genetic data, caste, religious or political beliefs, or any other category of data specified by the Authority. Additionally, fiduciaries are required to institute appropriate mechanisms for age verification and parental consent when processing sensitive personal data of children.
- **Transfer of data outside India:** Personal data (except sensitive personal data) may be transferred outside India under certain conditions. These include: (i) where the central government has prescribed that transfers to a particular country are permissible, or (ii) where the Authority approves the transfer in a situation of necessity.
- **Exemptions:** The Bill provides exemptions from compliance with its provisions, for certain reasons including: (i) state security, (ii) prevention, investigation, or prosecution of any offence, or (iii) personal, domestic, or journalistic purposes.
- **Offences and Penalties:** Under the Bill, the Authority may levy penalties for various offences by the fiduciary including (i) failure to perform its duties, (ii) data processing in violation of the Bill, and (iii) failure to comply with directions issued by the Authority. For example, under the Bill, the fiduciary is required to notify the Authority of any personal data breach which is likely to cause harm to the individual. Failure to promptly notify the Authority can attract a penalty of the higher of Rs 5 crore or 2% of the worldwide turnover of the fiduciary.
- **Amendments to other laws:** The Bill makes consequential amendments to the Information Technology Act, 2000. It also amends the Right to Information Act, 2005, and to permit non-disclosure of personal information where harm to the individual outweighs public good.