

The Ministry of Electronics and Information Technology of India has released a draft of the Personal Data Protection Bill, 2018 (Bill), which (when enacted) will significantly reshape the data privacy and protection landscape for organisations in India, as well as outside India, that have certain connections with India. Set forth below is a snapshot of the Bill, along with a brief analysis of its implications.

Applies:

- To government entities and private players
- To processing of personal data only
- If such data has been used, shared, disclosed, collected or otherwise processed in India
- To entities processing such data in connection with business carried on in India, irrespective of where the entity is located
- To any personal data collected, used, shared, disclosed or otherwise processed by any body corporate incorporated under Indian law or an Indian citizen, irrespective of whether it is actually processed in India

Exemptions:

- Few exemptions have been carved out, including processing data for research, archiving or statistical purposes, domestic purposes, journalistic purposes for certain types of entities

Summary of Key Provisions

Data protection is the safeguarding of personal information from corruption or loss. The Bill applies only for the purposes of data processing, which must be conducted in a fair and reasonable manner that respects the privacy of individuals. The Bill proposes to introduce a separate independent body, the Data Protection Authority of India (DPA) to enforce and regulate the implementation of the law. It also introduces rights for data principals (i.e., individuals whose personal data is involved), as well as obligations on data fiduciaries (i.e., entities or individuals who store, collect or process personal data).

Data principals would now have the right to confirmation and access. In addition, where personal data is inaccurate or misleading, data principals would have a right to correction. Similar to the European Union, the Bill seeks to introduce the “right to be forgotten,” which allows data principles to prevent continuing disclosure of personal data if such disclosure is no longer purposeful or is unlawful. However, it must be determined that such right overrides the right to freedom of speech or information.

For data fiduciaries, there are greater obligations now imposed on them by the Bill. For instance, there are limited grounds for processing of personal data, including for compliance with law, and on obtaining consent from individuals before their personal data can be processed. Such consent must be free, informed, specific, clear and capable of being withdrawn. Also, they are required to provide notice to the data principal at the time of collection of personal data, and such collection must be for purposes that are clear, specific and lawful. Enhanced safeguards have also been proposed for processing of personal data and sensitive personal data of persons below 18 years of age.

The Bill also governs the storage and cross-border transfer of personal data. Data fiduciaries are required to store at least one copy of personal data in data centers in India. Further, certain personal data categorized as critical may only be processed in India, and cannot be transferred outside of India except for emergency reasons such as the provision of health services. The cross-border transfer of non-critical personal data may be permitted on the basis of contractual terms and obligations, or as specified by the central government. Certain types of data fiduciaries that may have greater control over data are likely to be subject to additional compliances such as annual audits and mandatory appointment of a data protection officer.

In cases of data breach, data fiduciaries must notify the DPA in a timely manner, and in some circumstances, the data principal would also be notified depending on the severity of the breach. The Bill includes imprisonment as a punishment for any breach that significantly harms the data principal. As such, data fiduciaries should ensure that their data policies are compliant with the provision of the Bill.

Lastly, the Bill introduces the concept of “Privacy by Design,” which require data fiduciaries to have infrastructures in place to embed their obligations and avoid data breaches. For those who process data with risk of significant harm to the data principal, operating systems such as Trust Scores and Impact Assessments must be in place. With penalties ranging up to 4% of global turnover, entities affected should make efforts to ensure complete compliance with the impending data protection laws in India.

Existing Law and Implementation

The Bill essentially proposes to replace India's existing legal framework on personal data protection, which is currently enshrined in Section 43A (penalizing data controllers that cause wrongful loss or wrongful gain to any person), and Section 87 (which enables the existing rules on governing sensitive personal data), of the Information Technology Act, 2000. The Bill contemplates a phase-wise enactment with certain sections (relating to the DPA and the power to make rules and regulations) likely to be brought into effect immediately. The DPA is proposed to be set up in three months, with grounds for Processing Personal Data notified and codes of practice issued in 12 months. The operative provisions of the Bill are only to come into effect 18 months from the date of enactment.

Impact

The Bill is expected to introduce a number of significant changes to the existing general data protection regime in India. Complying with it will require Indian data fiduciaries to be aligned with global best practices on personal data. While individuals/data principals may have greater control over their personal data, the nature of obligations imposed on data fiduciaries may require these entities to re-evaluate their current practices on collection, storage and processing of personal data, as well as notice and consent requirements.

Contacts



Biswajit Chatterjee

Partner, Singapore
Co-chair, India Practice
T +65 6922 8664
E biswajit.chatterjee@squirepb.com



Kaustubh George

Senior Associate, Singapore
T +65 6922 8658
E kaustubh.george@squirepb.com



Anandee Banerji

Associate, Singapore
T +65 6922 8677
E anandee.banerji@squirepb.com

The contents of this update are not intended to serve as legal advice under Indian law, or legal advice related to individual situations or as legal opinions concerning such situations, nor should they be considered a substitute for taking legal advice.