

Highlights of Personal Data Protection Bill, 2019

Shri Ravi Shankar Prasad, Minister of Law and Justice, Communications and Electronics and Information Technology, has introduced 'The Personal Data Protection Bill, 2019' in the Lok Sabha. The bill has been referred to a Joint Parliamentary Committee for further examination. Committee shall submit a report in the House by the first day of the last week of the Budget Session, 2020.¹ The key provisions of the bill are summarised below:

1. **Horizontal Application:** The bill applies to both Government and private entities. [clause 2(A)(b)].

2. **Extra-territorial Application:** The applicability of the law will extend to data fiduciaries or data processors not present within the territory of India, if they carry out processing of personal data in connection with (a) any business carried on in India, (b) systematic offering of good and services to data principals in India, or (c) any activity which involves profiling of data principals within the territory of India. [clause 2 A(c)].

3. **Power to Exempt certain data processors:** The Central Government may, by notification, exempt from the application of this Act, the processing of personal data of data principals not within the territory of India. [Clause 37]

4. **Personal Data:** Personal data has been defined on the parameters of identifiability. The definition does not specifically mention any particular form of data or attribute, moreover such attributes maybe online or offline in nature. It shall also include any inference drawn from such data for the purpose of profiling; [clause 2 (28)]. The bill doesn't apply to 'Anonymised data' with respect to obligations and compliance requirements laid out in the bill. [clause 2(3)] However, the central Government is empowered to create policies to direct data fiduciaries or data processors to share Anonymised data or non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the central Government. [clause 91]

5. **Sensitive Personal Data:** Definition of sensitive personal data includes: (i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other data categorised as sensitive personal data under section 15. [clause 2(36)]

6. **Obligations of Data Fiduciary:** This chapter lays down the fundamental principles of the bill as: a) Presence of specific, clear and lawful purpose, b) Limitation on purpose, c) Limitation on collection, d) Notice, e) Data Quality, f) Restriction on retention and g) Accountability. [Chapter II]

7. **Grounds for Processing Personal Data:** The legal grounds for processing under the bill include: (a) consent, (b) functions of state, (c) compliance with law or order of court/tribunal, (d) for prompt action in case of individual medical emergencies or in case of public health emergency, (e) purposes related to employment and (f) reasonable purposes of the data fiduciary. [Chapter III]

8. **Processing Sensitive Personal Data:** The legal ground for processing SPD under the bill is restricted to explicit consent alone. [clause 11 (3)]

¹ [Access here.](#)

9. Personal and Sensitive Personal Data of Children: Processing of personal and sensitive personal of children by data fiduciaries should be done in a manner that protects and is in best interests of the child. Data fiduciaries are required to establish mechanisms for age verification and parental consent. Fiduciaries that operate commercial websites or online services directed at children or process large volume of children personal data would be classified as guardian data fiduciaries and barred from performing certain processing operations. [clause 16]

10. Data Principal Rights: The bill provides the data principal with the (a) right to confirmation and access, (b) correction and erasure, (c) data portability and (d) right to be forgotten. [chapter V]

11. Transparency and Accountability Measures: The bill lays down practices that regulated entities under the bill must implement. These include: (a) Privacy by design policy, (b) data protection impact assessment, (c) maintenance of records, (d) appointing a data protection officer and (e) data audits. Practices inscribed in (b) to (e) are to be carried about by data fiduciaries which have been classified as “significant data fiduciaries” by the Data Protection Authority. If the authority categories a fiduciary as a “Social media intermediary”, then such entity would have to provide the user a voluntary verification mechanism. [chapter VI]

12. Restriction on and conditions for transfer of Personal Data Outside India: Clause 33 lays down that sensitive personal data shall continue to be stored in India, but data can be transferred outside the territory of India under the conditions laid down under clause 34. These conditions are provision of explicit consent by the data principle, and contract for transfer, or intra group scheme, or adequacy decision or a transfer that is green lit by the authority for a specific purpose. Data that is classified as ‘critical personal data’ by the central Government shall be processed only in India but may be transferred outside India in case of emergency situations for prompt action; such transfers need to be notified to the authority. Critical data may also be transferred to a country/territory that has secured an adequacy decision from the central Government, unless such transfer may prejudice security or some national strategic interest of the state.

13. Data Protection Authority of India: The bill establishes an independent authority empowered to oversee the enforcement of the bill. The adjudication process will be looked after by the adjudication officers appointed by the Authority. [clause 41]

14. Penalties, Remedies and Offences: The bill lays down penalties under chapter X of the bill, ranging from five crore rupees or two per cent of total worldwide turnover to fifteen crore rupees or 4% of the total worldwide turnover. The Data principal under clause 64 has the remedy to claim compensation for harm suffered as a result of any violation of any provision in the bill from the data fiduciary or the data processors. The bill inscribes certain offences under chapter XIII of the bill, which are punishable with imprisonment.

15. Omissions: Section 43A and section 87 of the Information Technology Act, 2000 shall be repealed.

.....

1. The Personal Data protection Bill, 2019, [access here](#).