Highlights of Personal Data Protection Bill, 2018

The committee of experts under the chairmanship of Justice B.N. Srikrishna, has brought its deliberations to a close and handed over the draft protection of personal data bill for India to Ministry of electronics and information technology for circulation. The following summarises the key provisions of the bill:

1. **Change in terminology:** The known terms of references, i.e., "Data Subject" and "Data Controller", have been reformulated as "Data Principal" and Data Fiduciary", to emphasize greater accountability and trust between the two. **[Section 3(13), Section (14)]**

2. **Horizontal Application:** The proposed bill applies to both government and private entities. **[Section 2(1)(b)]**

3. **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 principles in India, or (c) any activity which involves profiling of data principals within the territory of India. **[Section 2 of the Bill]**

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. **[Section 3 (35)].** The bill expressly mentions the exclusion of anonymized data from the application of the law. **[Section 2(3) of the Bill]**

5. **Sensitive Personal Data:** Definition of sensitive personal data as it existed under SPDI Rules[1], has been expanded to include passwords; 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. **[Section 3(35) of the bill]**

6. **Grounds for Processing Personal Data:** The legal ground 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 emergencies, (e) purposes related to employment and (f) reasonable purposes of the data fiduciary. **[Chapter III]**

7. **Grounds for Processing Sensitive Personal Data:** The legal grounds for processing SPD under the bill include: (a) explicit consent, (b) functions of state, (c) compliance with law or order of court/tribunal, (d) for prompt action in case of emergencies for passwords, financial data, health data, official identifiers, genetic data, and biometric data. **[Chapter IV]**

[1] Rule 3. Sensitive personal data or information.— Sensitive personal data or information of a person means such personal information which consists of information relating to;— (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information.

8. **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 advances the rights and 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. **[Section 23 of the Bill]**

9. **Data Principal Rights:** The bill provides the data principal with the (a) right to confirmation and access, (b) correction, (c) data portability and (d) right to be forgotten. **[Section 24, Section 25, Section 26, Section 27 of the Bill]**

10. **Transparency and Accountability Measures:** Chapter VII of the bill lays down practices that regulated entities under the bill must implement. These include: (a) Privacy by design, (b) data protection impact assessment, (c) record keeping, (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 can been classified as "significant data fiduciaries" by the Data Protection Authority.

11. **Transfer of Personal Data Outside India:** Section 40 under the bill places restrictions on cross-border data flows. Section 40 (1) mandates storing one serving copy of all personal data within the territory of India. While section 40 (2) empowers the central government to classify any sensitive personal data as critical personal data and mandate its storage and processing exclusively within India.

12. **Conditions for Transfer of Personal Data Outside India:** The transfer is made subject to standard contractual clauses or intra-group schemes that have been approved by the Authority, prescribed that transfers to a particular country, or to a sector within a country or to a particular international organisation is permissible by the central government, transfers permissible due to a situation of necessity, consent with respect to personal data and explicit consent with respect to sensitive personal data. These provisions do not extent to critical personal data. **[Section 41 of the bill]**

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 wing of the Authority. **[Chapter X. Section 60]**

14. **Penalties, Remedies and Offences**: The bill lays down penalties under chapter XI 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 principle under section 75 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. Transition Provisions: Section 97 of the bill provides a structured timeline for enforcement from the date enacted of act. The enforcement duration is 18 months from the date of enactment, other than section 40, the duration of enforcement for this provision would be notified by the central government.

***

The Personal Data Protection Bill, 2018 can be accessed here : http://meity.gov.in/content/personal-data-protection-bill-2018.

Data Protection Framework and committee Report can be downloaded here: http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf