NASSCOM®

DSCI PROMOTING DATA PROTECTION

Protection of Personal Data 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. Area on restrictions around cross border flow of data which are immediately apparent are highlighted. Text in *italics* is reproduced from the Bill.

- **Personal data**: A copy of all personal data is required to be stored in India. There are restrictions on transferring personal data outside India.
- **Sensitive personal data**: Passwords, financial data and official identifier are being treated as sensitive personal data. Sensitive personal data has to be only stored in India barring some exceptions. It can only be transferred out of India for provision of health services or emergency services where such transfer is strictly necessary, or to a particular country, a prescribed sector within a country or to a particular international organisation where the Central Government is satisfied that such transfer or class of transfers is necessary and does not hamper the effective enforcement of this Act.
- **Critical personal data**: The Government has the power to notify critical personal data which would be required to be processed only in a server in India. This suggests that such data needs to be stored as well as processed only in India.
- **Criminal Offence**: Offences under the Act, including those related to personal data, are treated as criminal offences.
- **Anonymised data**: The Bill does not apply to processing of anonymised data.
- **Date of restrictions on data flow coming into force**: The Bill leaves it to the Government to decide when to notify the restriction on cross border flow of data including requirement to store a copy of personal data in India.

---

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 annoymised 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]**

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. Section 41(1) allows personal data to be transferred outside India where:

    (a) the transfer is made subject to standard contractual clauses or intra-group schemes that have been approved by the Authority; or

[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.

(b) the Central Government, after consultation with the Authority, has prescribed that transfers to a particular country, or to a sector within a country or to a particular international organisation is permissible; or

(c) the Authority approves a particular transfer or set of transfers as permissible due to a situation of necessity; or

(d) in addition to clause (a) or (b) being satisfied, the data principal has consented to such transfer of personal data; or

(e) in addition to clause (a) or (b) being satisfied, the data principal has explicitly consented to such transfer of sensitive personal data, which does not include the categories of sensitive personal data notified under sub-section (2) of section 40.

(2) The Central Government may only prescribe the permissibility of transfers under clause (b) of sub-section (1) where it finds that the relevant personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements, and the effectiveness of the enforcement by authorities with appropriate jurisdiction, and shall monitor the circumstances applicable to such data in order to review decisions made under this sub-section. **[Section 41(1) of the bill]**

12. **Transfer of Sensitive Personal Data outside India: Sensitive personal data has to be only stored in India barring some exceptions**. It can only be transferred out of India for provision of health services or emergency services where such transfer is strictly necessary, or to a particular country, a prescribed sector within a country or to a particular international organisation where the Central Government is satisfied that such transfer or class of transfers is necessary and does not hamper the effective enforcement of this Act. *Sensitive personal data notified by the Central Government may be transferred outside the territory of India—*

(a) to a particular person or entity engaged in the provision of health services or emergency services where such transfer is strictly necessary for prompt action under section 16; and

(b) to a particular country, a prescribed sector within a country or to a particular international organisation that has beenprescribed under clause (b) of sub-section (1), wherethe Central Government is satisfied that such transfer or class of transfersis necessary for any class of data fiduciaries or data principals anddoesnot hamper the effective enforcement of this Act. **[Section 41(3) of the bill]**

13. **Transfer of Critical Data outside India**: Section 40 (2) empowers the central government to classify any sensitive personal data as critical personal data and mandate its processing exclusively within India. (Note: This suggests that storing will also be only in India as critical data is presumably more sensitive than sensitive data.)

12. **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]**

13. **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. Offences related to personal data can invite imprisonment up-to 3 years and those related to sensitive personal information can invite imprisonment up-to 5 years.

14. **Transition Provisions:** Section 97 of the bill provides a structured timeline for enforcement from the date enacted of act. The Bill provides 12 months for the Authority to notify the ground of processing personal data for prevention/ detection of unlawful activity, recovery of debt, credit score etc and code of practices for data quality, storage, processing of personal and sensitive personal data etc. The provisions of the Bill are required to come into force within 18 months of enactment. This potentially can leave just 6 months for the industry to gear up for implementation.

15. **Transitional provisions related to data localization**: The date of coming into force of section 40 dealing with restrictions on cross border flow of data has not been provided in the Bill. It has been left to the Central Government to decide.