

## BACKGROUND

The Supreme Court of India has upheld the right to privacy of an individual as a fundamental right flowing from the right to 'life and personal liberty' under the Indian Constitution. To uphold and protect this right, the Government of India ("GoI") has introduced the Personal Data Protection Bill, 2019 ("Privacy Bill"), which is in line with the EU General Data Protection Regulation ("EU GDPR"). The Privacy Bill is yet to become a law.

We have provided below some of the relevant aspects of the Privacy Bill through Q&A. However, please note that the Privacy Bill has other incidental and ancillary clauses which are not covered. For specific query, please write to us and we will provide relevant response.

### 1. The Privacy Bill once becomes a law will be applicable to whom?

The Privacy Bill will be made applicable to processing of "personal data" by:

- (i) Government,
- (ii) Indian company,
- (iii) any citizen of India,
- (iv) any person(s) created under Indian law;
- (v) companies incorporated in India, and
- (vi) foreign entities, if such processing is in connection with:
  - a. any business carried on in India,
  - b. any systematic activity of offering goods or services to individuals within the territory of India; or
  - c. in connection with any activity which involves profiling of individual within the territory of India.

For a foreign entities to be covered under the Privacy Bill, factors such as the use of a local language or a currency of India, possibility of ordering goods and services in that language, or the mentioning of customers or users who are in the India by such foreign entity will be considered.

**"Processing"** in relation to personal data, means:

- operation(s) performed on personal data, and
- Includes operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

**Data Fiduciary:** The entity who determines the purpose and means of processing of personal data.

**Data Processor:** Any person who processes personal data on behalf of a data fiduciary.

**Data Principle:** The natural person to whom the personal data relates.

### 2. What types of data are covered under the Privacy Bill?

The Privacy Bill protects 3 types of data, (a) personal data, (b) sensitive personal data, and critical personal data.

---

---

**Personal Data** has been defined to include data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual.

The Privacy Bill categorises certain personal data as sensitive personal data. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government, in consultation with the Authority and the concerned sectorial regulator.

Certain personal data is also categorised as critical personal data. What constitutes critical personal data will be notified by the Government from time to time.

### 3. **What are the general obligations of the data fiduciary?**

Main obligation of data fiduciary are:

- (i) personal data can be processed only upon the consent from the data principal;
- (ii) data to be processed for specific, clear and lawful purpose only;
- (iii) in a fair and reasonable manner and ensure the privacy of the data principal;
- (iv) for the purpose consented to by the data principal;
- (v) data to be collected only to the extent that is necessary for the purposes;
- (vi) implement security safeguards (such as data encryption and preventing misuse of data);
- (vii) conduct age verification and parental consent, where data principal is minor;
- (viii) delete personal data at the end of processing;
- (ix) at the time of collection of the personal data, give notice to the data principal of:
  - purpose of collection,
  - nature of data collected,
  - contact details of data fiduciary,
  - right to withdraw consent,
  - consequences of the failure to provide such personal data,
  - information regarding any cross-border transfer,
  - the period for which the personal data shall be retained,
  - procedure for grievance redressal,
  - rights of data principal, and
  - any other information as may be specified by the regulations.

### 4. **What are the rights of data principal?**

The data principal has rights to:

- (i) obtain confirmation from the fiduciary on whether their personal data has been processed,
- (ii) seek correction of inaccurate, incomplete, or out-of-date personal data,
- (iii) have personal data transferred to any other data fiduciary in certain circumstances, and
- (iv) restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn.

### 5. **Can personal data be used without the consent of the data principal?**

In certain circumstances, personal data can be processed without consent of the data principal, these include:

- (i) if required by the State for providing benefits to the individual;
- (ii) required under any law for the time being in force;
- (iii) for compliance with any order or judgment in India;

- 
- (iv) to respond to a medical emergency;
  - (v) to ensure safety/provide assistance during any disaster or any breakdown of public order;
  - (vi) (other than sensitive personal data) where data fiduciary is an employer of data principal for the purpose of recruitment/termination/other benefits and employee related issues;
  - (vii) processing is required for reasonable purposes specified by regulations/law.

In addition to the above, the Central Government may direct data fiduciaries to provide it with any: (i) non-personal data, and (ii) anonymised personal data (where it is not possible to identify data principal) for:

- (i) better targeting of delivery of services; and
- (ii) formulation of evidence-based policies by the Central Government.

## **6. What are the various safeguard measures that the data fiduciary are required to put in place?**

The Privacy Bill requires the data fiduciary to put in place certain safeguard measures, these to include:

- (i) Privacy by design policy to be certified by Data Protection Authority of India. The policy to containing details of:
  - a. managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal;
  - b. obligations of data fiduciaries;
  - c. technology used in the processing of personal data;
  - d. legitimate interests of businesses;
  - e. protection of privacy throughout processing process;
  - f. processing in a transparent manner; and
  - g. protecting the interest of the data principal.
- (ii) implement necessary security safeguards, including de-identification and encryption;
- (iii) data protection impact assessment to be conduct before use of such new technologies;
- (iv) require policies and the processing conduct to be audited annually by an independent data auditor;
- (v) appoint a data protection officer to advice the data fiduciary, monitor personal data processing activities, provide other assistance and co-operation to the Data Protection Authority; and
- (vi) provide mechanisms to redress the grievances of data principals.

## **7. Where personal data can be stored?**

Sensitive personal data is required to be stored in India.

Sensitive personal data can be taken outside India for the purpose of processing, when explicit consent is given by the data principal, and such transfer is pursuant to a contract or intra-group scheme approved by the Data Protection Authority.

The critical personal data is required to be processed only in India. What constitutes critical personal data will be notified by the Government from time to time.

---

8. **Is there any authority responsible to regulate and oversee the enforcement of data privacy?**

The Privacy Bill provides for a Data Protection Authority. This authority has the power to:

- (i) take steps to protect interests of individuals,
- (ii) prevent misuse of personal data, and
- (iii) ensure compliance with the Bill.

9. **Does the Privacy Bill allows any exception or exemption from its applicability?**

**Exemption for Government Agency:** The central government has the power to exempt any agency of Government from application of the Privacy Bill:

- (i) in interest of security of state, public order, sovereignty and integrity of India and friendly relations with foreign states, and
- (ii) for preventing incitement to commission of any cognisable offence relating to the above matters.

**Exemption for certain specific purpose:** Certain provisions of the Privacy Bill is exempted where personal data is processed for:

- (i) prevention, investigation and prosecution of any offence,
- (ii) enforcement of legal right,
- (iii) judicial function,
- (iv) personal and domestic purpose,
- (v) journalistic purposes, and
- (vi) necessary for research, archiving, or statistical purposes

However, such processing must be for a specific, clear and lawful purpose, with certain security safeguards.

10. **What are the penalties for breach of the provisions of Privacy Bill?**

Penalty for some of the breaches under the Privacy Bill are:

- (i) processing or transferring personal data in violation of the law is punishable with a fine which may extend to INR 15,00,00,000 (USD 2.1 million approx.) or 4% of the worldwide turnover of the preceding financial year, whichever is higher;
- (ii) failure to (i) take prompt and appropriate action on data security breach, (ii) undertake a data protection impact assessment, (iii) conduct a data audit, and (iv) appoint a data protection officer, are punishable with fine which may extend to INR 5,00,00,000 (USD 700,000 approx.) or 2% of its total worldwide turnover of the preceding financial year, whichever is higher; and
- (iii) re-identification and processing of de-identified personal data without consent is punishable with imprisonment of up to three years, or fine, which may extend to INR 2,00,000 (USD 2800 approx.) or both.

**“Total worldwide turnover”** means the gross amount of revenue recognised in the profit and loss account or any other equivalent statement, as applicable, from the sale, supply or distribution of goods or services or on account of services rendered, or both, and where such revenue is generated within India and outside India.