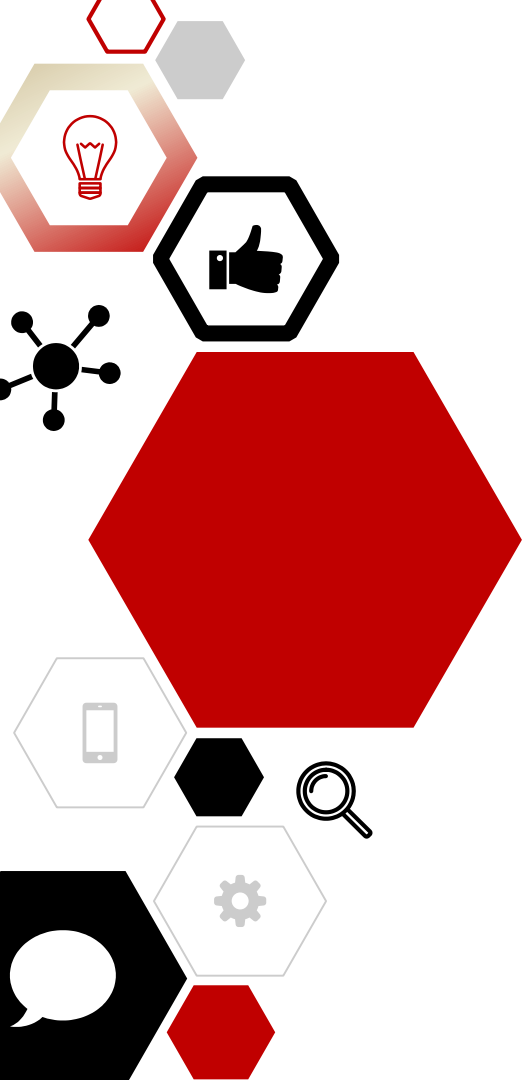
18 October 2018

Introduction to Personal Data Protection Bill

The Personal Data Protection Bill, 2018

- The Personal Data Protection Bill, 2018 and the report of Srikrishna Commission on data protection have been submitted by Justice Srikrishna panel to the Ministry of Electronics and Information Technology.
- The committee has suggested measures to protect personal information of citizens, the role and duties of data processors and the rights of individuals.



Objects

- To **protect personal data** as an essential facet of informational privacy.
- To create a **free and fair digital economy.**
- To create a relationship of **trust** between persons and entities processing their personal data.
- To create a framework for implementing **organizational and technical measures** in processing personal data.
- To lay down **norms for cross-border transfer** of personal data.
- To **provide remedies** for unauthorised and harmful processing.
- To establish a **Data Protection Authority** for overseeing processing activities.

Important Definitions

Personal data means data relating to a natural person having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person

Sensitive Personal Data means personal data revealing passwords, financial data, health data, sexual orientation, genetic data, transgender status, caste or tribe;

Data fiduciary means any person, including the State, a company, any juristic entity or any individual who determines the purpose and means of processing of personal data

Processing in relation to personal data includes operations such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction

De-identification means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal

Data principal means the natural person to whom the personal data relates.

Data processor

- means any person, the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary
- but does not include an employee of the data fiduciary

Applicability

As per S.2, the Act will apply to the following:

(i) Where **such personal data** has been collected, disclosed, shared or otherwise **processed within the territory of India and**

(ii) Where **such personal data is processed by** the State, **any Indian company**, any Indian citizen or any person or body of persons **incorporated or created under Indian law**.

Authority as per the Bill

The Central Government shall, by notification, establish

- Data Protection Authority of India [Section 49]
- Appellate Tribunal [Section 79]

About the Proposed Bill

- It strikes a balance between privacy and the need to allow data to be used for legitimate purposes.
- It places a great degree of responsibility on data fiduciary.
- Journalists will be exempted as will not be required to seek consent while collecting sensitive personal data.
- Companies that design to de-identify data will not be exempted.
- The practical and technical challenges of implementing multi-layered consent framework is difficult and time consuming as well as costly.
- Business will have to entirely re-organise their process to accommodate the new requirement.
- Data fiduciary will have to insist on interspersing additional steps to demonstrate that they had sought full and informed consent.
- Govt. can declare any data as critical at any point of time and ask for exclusive data localisation in India.
- Criminal Prosecution as per the proposed bill is very stringent.

Salient Features of the Bill

Consent of Data Principal

When consent mandatory

- Personal data may be processed on the basis of the consent of the data principal.
- Consent must be free, informed, specific, clear and capable of being withdrawn.

When consent not mandatory

- Processing of personal data for functions of the State.
- Processing of personal data in compliance with law or any order of any court or tribunal.
- Processing of personal data necessary for prompt action.
- Processing of personal data necessary for purposes related to employment.
- Processing of data for reasonable purposes.

Lawful Processing

While processing personal data or sensitive personal data, consent of the data principal is required.

Personal Data [S.12]

- Personal data may be processed on the basis of the consent of the data principal.
- Consent must be free, informed, specific, clear and capable of being withdrawn.

Sensitive Personal Data [S.18]

- Sensitive personal data may be processed on the basis of **explicit consent.**
- Consent must be free, informed, specific, clear and capable of being withdrawn.

Personal Data Breach

The data fiduciary shall **notify the Authority of any personal data breach** where such breach is likely to cause harm to any data principal.

Grievance Redressal

Every data fiduciary shall have in place **proper procedures and effective mechanisms to address grievances** of data principals efficiently and in a speedy manner.

Notice

While processing personal data, the data fiduciary shall provide the data principal with the following information:

- The **purposes** for which the personal data is to be processed
- The **categories** of personal data being collected
- The **identity and contact details of the data fiduciary and** the contact details of the data **protection officer**(if applicable)
- The **right of the data principal** to withdraw such consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent
- The **consequences of the failure** to provide such personal data
- The **source of such collection**, if the personal data is not collected from the data principal

- The individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable
- The **period for which the personal data will be retained** or where such period is not known, the criteria for determining such period
- The existence of and procedure for the **exercise of data principal rights**
- The procedure for **grievance redressal** u/S.39
- The existence of a **right to file complaints** to the Authority
- Any **other information** as may be specified by the Authority.

Privacy by Design

Every data fiduciary shall implement policies and measures to ensure that the managerial, organizational, business practices and technical systems are designed in a manner to anticipate, identify and avoid harm to the data principal.

Transparency

The data fiduciary shall take reasonable steps to maintain transparency for processing of data.

Security Safeguards

- The data fiduciary and the data processor shall **implement appropriate security safeguards**
- **Undertake a review** of its security safeguards periodically as may be specified
- **Take appropriate measures** accordingly.

Record-Keeping

The data fiduciary shall maintain accurate and up-to-date records and these records shall be maintained in such form as specified by the Authority.

Processing by entities other than data fiduciaries

- The data fiduciary shall only engage, appoint, use or involve a data processor to process personal data on its behalf through a valid contract.
- The data processor shall not further engage, appoint, use, or involve another data processor except with the authorization of the data fiduciary, unless permitted through the contract.
- The data processor shall treat any personal data that comes within their knowledge as confidential.

Data Audits

The data fiduciary shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor under this Act.

Data Protection Officer

The data fiduciary shall appoint a data protection officer. He will perform the following functions:

- Provide information and advice to the data fiduciary
- Monitor personal data processing activities to ensure that such processing does not violate the provisions of this Act
- Provide assistance to the Authority on matters of compliance of the data fiduciary with provisions under this Act
- Act as the point of contact for the data principal for the purpose of raising grievances
- Maintain an inventory of all records maintained by the data fiduciary

Offences

Provisions	Contravention	Punishment or Fine
S.90	Obtaining, transferring or selling of personal data contrary to the Act	Imprisonment for a term not exceeding **three years** or shall be liable to a fine which may extend up to **rupees two lakh or both**
S.91	Obtaining, transferring or selling of sensitive personal data contrary to the Act	Imprisonment for a term not exceeding **five years** or shall be liable to a fine which may extend up to **rupees three lakhs or both.**
S.92	Re-identification and processing of de-identified personal data	Imprisonment for a term not exceeding **three years** or shall be liable to a fine which may extend up to **rupees two lakh or both.**
S.95	Offences by companies	The person responsible for management shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly

Penalties

Section	Contravention by Data Fiduciary		Penalty
69(1)	**Contravening Provision**	**Contravention**	Penalty which may extend up to five crore rupees or two per cent of its total worldwide turnover of the preceding financial year, whichever is higher
	S.32	Failure to take prompt and appropriate action in response to a data security breach	
	S.33	Failure to undertake a data protection impact assessment by a significant data fiduciary	
	S.35	Failure to conduct a data audit	
	S.36	Failure to appoint a data protection officer	
	S.38(2)	Failure to register with the Authority	

Section	Contravention		Penalty
	Contravening Provision/Provisions of Chapter	**Contravention**	
69(2)	Chapter II	Violation of Data Protection Obligations	Penalty which may extend up to fifteen crore rupees or four per cent of its total worldwide turnover of the preceding financial year, whichever is higher.
	Chapter III	Processing of personal data in violation of the provisions	
	Chapter IV	Processing of sensitive personal data in violation of the provisions	
	Chapter V	Processing of personal data of children in violation of the provisions	
	S.31	Failure to adhere to security safeguards	
	S.41	Transfer of personal data outside India	

Section	Contravention	Penalty
S.70	Failure to comply with data principal requests under Chapter VI (Data Principal Rights)	Penalty of five thousand rupees for each day during which such default continues, subject to a maximum of ten lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.
S.71	Failure to furnish report, returns, information, etc	Penalty which shall be ten thousand rupees for each day during which such default continues, subject to a maximum of twenty lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.

Section	Contravention	Penalty
S.72	Failure to comply with direction or order issued by the Authority	In case of a data fiduciary may extend to twenty thousand rupees for each day during which such default continues, subject to a maximum of two crore rupees. In case of a data processor may extend to five thousand rupees for each day during which such default continues, subject to a maximum of fifty lakh rupees.
S.73	Contravention where no separate penalty has been provided	Penalty subject to a maximum of one crore rupees in case of significant data fiduciaries, and a maximum of twenty five lakh rupees in all other cases .

Thanks!

Any questions?

You can reach us at:

- admin@thinkinglegal.in