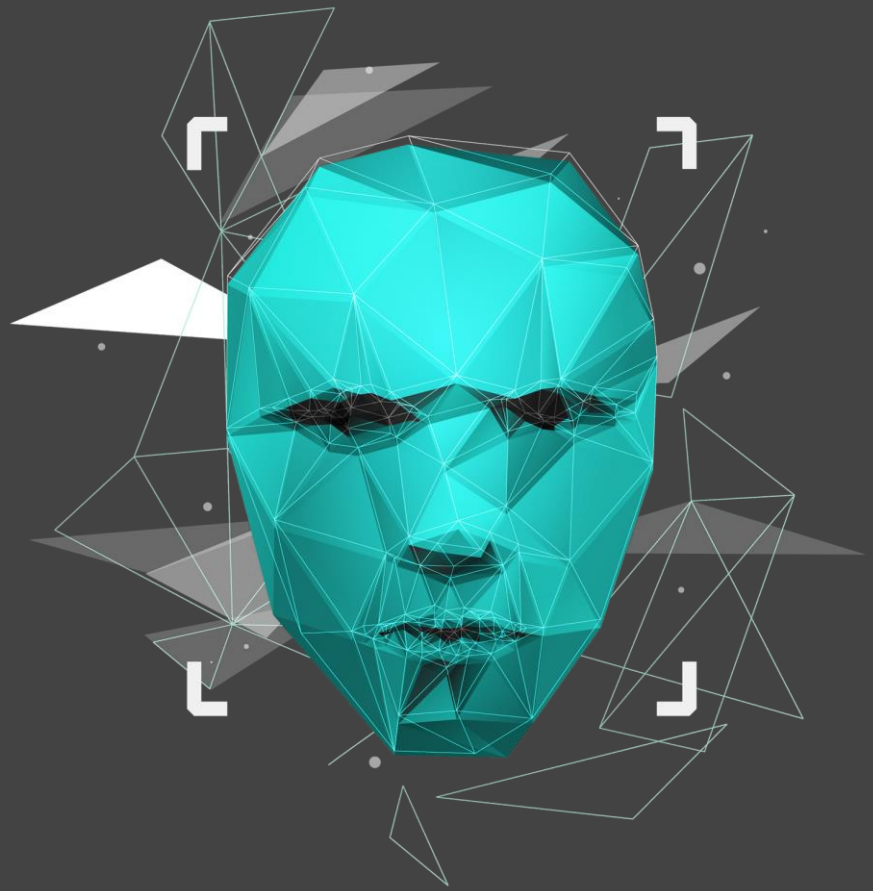
Personal Data Protection Bill 2019

An introduction, analysis, & comparison



SIGNZY

Background

- In India, a regulation governing data privacy and data protection is set to be passed this year.
- The need stemmed from the 2017 Supreme Court judgement on the Right to Privacy.
- A draft data protection bill was then composed by a committee headed by Justice B. N. Srikrishna.
- After about 2 years of contentious debate on the bill, during which it was floated for public feedback from stakeholders, it was tabled in the Indian Parliament on 11 December 2019.
- Currently, a joint parliamentary committee is scrutinizing the revised draft of the bill, codified as the Personal Data Protection Bill 2019 (PDP Bill).
- Post this, it will be debated in the Indian Parliament and finally passed.

SIGNZY

Why do we need a PDP Bill?

01 To provide protection of privacy to individuals

02 To create accountability of entities processing personal data

03 To provide redressal mechanisms for unauthorised and harmful processing

SIGNZY

Applicability of Bill

It is to govern personal data processed by:

01	02	03
The government	Companies incorporated in India	Foreign companies dealing with personal data of individuals in India

SIGNZY

What is personal data?

Personal data is data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual.

Types of personal data

- **Sensitive personal data:** This includes financial data, biometric data, caste, religious or political beliefs, health data, sex life/intersex status, sexual orientation/transgender status
- **Critical personal data:** Categories of personal data to be notified by the Central Government in the future.

SIGNZY

Key Definitions

Data principal

Citizens whose personal data is being processed or “the natural person to whom the data belongs”

Data fiduciary

Entities that process the personal data or “any person or legal entity including the State who determines the purpose and means of processing the data”

Data processor

Any person or legal entity including the State who processes the data. This may consist of the data controller or data fiduciary itself or a third party.

SIGNZY

Data Processing

Data localisation requires the collection, processing, or storage of certain types of data within the borders of the nation where the data was generated, before being internationally transferred.

- Sensitive personal data: This category of data when collected, shared or disclosed to the data fiduciary in India has to be stored only within the borders of the State. It may be transferred beyond the territory of India for processing, subject to explicit consent and conditions.
- Critical personal data: Strict data localization norms exist for this category of data. It can only be processed within the borders of India. The problem arises since this type of data has not been defined yet.

SIGNZY

Rights guaranteed

- The right to obtain confirmation from the fiduciary on whether their personal data has been processed
- The right to seek correction of inaccurate, incomplete, or out-of-date personal data
- The right to have personal data transferred to any other data fiduciary in certain circumstances
- The right to restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn.
- Right to be forgotten

Rights not guaranteed

- Right to restrict processing: The GDPR grants the data principle the right to limit the processing of their data. This means that the processing of personal data can be stalled at an intermittent stage. This can be requested on the grounds of unlawful processing, data inaccuracy etc. The PDP Bill doesn't guarantee this right.
- Right to not be subjected to automated decisions: The GDPR grants the right to not be subjected to automated decision-making, such as profiling. The PDP Bill does not ascertain this right.

SIGNZY

Responsibility of Data Fiduciaries

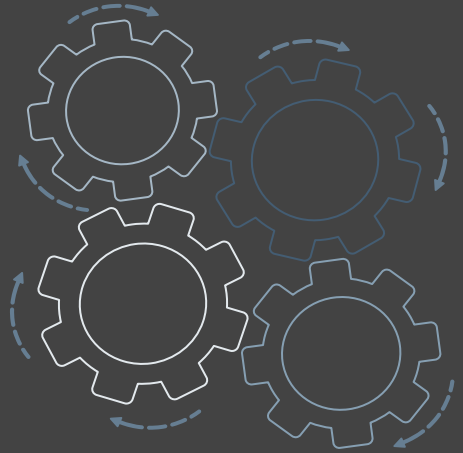
- Personal data can be processed only for specific, clear and lawful purpose
- All data fiduciaries must undertake certain transparency and accountability measures such as:
  - Implementing security safeguards (such as data encryption and preventing misuse of data)
  - Instituting grievance redressal mechanisms to address complaints of individuals

- They must institute mechanisms for age verification and parental consent when processing sensitive personal data of children
- The PDP Bill 2019 introduces the concept of a Privacy by Design policy. Every data fiduciary is required to prepare a privacy by design policy and have it certified by the Data Protection Authority

SIGNZY

Privacy By Design

The Privacy By Design (PbD) measures in the bill mandate:



- Embedding privacy into business processes and technologies
- Submitting a PbD policy to the Authority for certification
- Availability of a certified PbD policy on the data fiduciary's website.

SIGNZY

Compliance norms	Definition
Informed Consent	Personal data shall only be processed after explicit consent given by the data principal at the commencement of its processing.
Specific Purpose	Personal data shall be collected only to the extent that is necessary for the purposes of processing. This means that it cannot be collected for reasons that are not known or declared.
Data Erasure	Personal data must be erased after the purpose for which it was shared has been met. The data principal has the right to ask for the erasure of their personal data.
Data Portability	When the processing of the personal data has been carried out through automated means, the data principal has the right to receive a copy of their personal data in a structured, commonly used and machine-readable format.

SIGNZY

Compliance Practices (Part I)

No.	Category	Compliance Step	Signzy's Recommended Architecture
1	**Data Minimization**	Collect only required data	The flow is dynamically structured to collect only the required data from each person.
2	**Encryption**	Encrypt all Personal Data	All data communication channels are encrypted
3	**Purpose Limitation**	Use it only for the purpose intended	Data is stored on-premise. Only the data controller has access to the data
4	**Data Processing**	Only process personal data on instructions from the controller	The data is only accessible by the controller. The controller has full transparency of all the processing that takes place,
5	**Compliance Audits**	Enable and contribute to compliance audits	Conduct regular audits and be ISO compliant
6	**Data Breach**	Notify immediately on data breaches	You should inform your customers immediately in case of any data breach
7	**Geographic Limitation**	Restrict personal data transfer to a third country	We provide the flexibility to store data in whichever country required

SIGNZY

Compliance Practices (Part II)

No.	Category	Compliance Step	Signzy's Recommended Architecture
8	**Data Access**	Right of access by the data subject	Any person who has personal data in the system can view their own data but every such communication has to pass through the controller
9	**Erasure**	Right to be forgotten	Provide an option to delete all data belonging to a user and any identifier related to the data
10	**Accuracy**	Personal data shall be accurate and, where necessary, kept up to date	The data collected through the controller can not be modified because they pass through encrypted channels only. We also provide an option to the controllers to refresh all data of an individual periodically
11	**Transparency and Modalities**	Transparent information, communication, and modalities for the exercise of the rights of the data subject	Every step in the process is clear about the data being collected at that step and measures are taken to ensure that the person has complete knowledge of the entire process

SIGNZY

Compliance Practices (Part III)

No.	Category	Compliance Step	Signzy's Recommended Architecture
12	**Integrity and Confidentiality**	Ensures appropriate security and protection against accidental loss	The data can not be modified by anybody other than the controller. To prevent accidental loss, we maintain an archive/backup of all data in an encrypted format.
13	**Consent**	User Consent is taken before collecting any personal data	User consent is taken at every step while clearly stating the intent on collecting their personal data.
14	**Purpose Limitation**	Use it only for the purpose intended	Data is stored on-premise. Only the data controller has access to the data
15	**Storage Limitation**	Personal data should be kept for no longer than is necessary for the purposes	The data should be deleted as soon as the intended purpose is fulfilled

SIGNZY

Concerns for Tech Companies

With companies preparing to adapt to the new compliance requirements, there are growing concerns for tech companies:

- Mounting operational expenses
  - Compliance constraints
    - Rising cost of doing business
      - Increase in barriers to entry

This could limit the ability of new competitors to enter the market. Restrictions on sharing data with third parties could make it difficult for companies to collaborate on data-driven innovation.

SIGNZY

Provisions for companies working on innovative data driven tech

The PDP introduces the concept of a “sandbox”.

- It gives the Data Protection Authority the power to modify provisions for certain data fiduciaries that work for “innovation in artificial intelligence, machine-learning or any other emerging technology in public interest”.

- Under Section 40 of the PDP bill, the exemptions that may be given as part of the sandbox include required relaxations. This includes specifications of clear purpose for data processing and collection, and the limits to the period of data retention.

SIGNZY

Controversial Aspects

The bill gives the central government the power to exempt its agencies from the purview of this act. The purpose of revoking the regulations are vaguely defined. It can be:

a. in the interest of sovereignty and integrity of India or
b. to preserve national security

This thereby eliminates the obligations of consent, accountability and transparency to ensure fair processing of data.

It is yet to be determined whether the Indian PDP Bill is closer to the EU's progressive GDPR or to China's policy of control. Either way, it has managed to irk both Big Tech companies and privacy advocates alike. Companies with data banks aren't happy with the cost and hassle of compliance. They deem the bill as isolationist due to its restrictive certification requirements to operate in India. Privacy advocates highlight how the exceptions in the bill can lead to State excesses of control over our data.

SIGNZY

Introducing GDPR

- The European Union set precedence with the European General Data Protection Regulation (GDPR).
- The GDPR was adopted in 2016 and enforced on 25 May 2018. It is not a mere directive, but a regulation. This implies that it is directly binding and applicable although it does allow for some flexibility to individual member nations to adjust the provisions.
- The GDPR is also not an Act, which means that its members have passed their own legislations based on the regulation.

SIGNZY

GDPR vs PDP Bill

- The aim of data protection frameworks is to protect the data while safeguarding its free flow. The GDPR has no hard data localization conditions. It allows for cross-border transfer of all types of data if the country of data transfer has an adequate framework of data protection. India's PDP has different data localization needs for different types of data as explained earlier.
- The GDPR grants the data subject the right to limit the processing of their data. It grants the right to not be subjected to automated decision-making, such as profiling. The PDP Bill does not grant these rights.
- The GDPR lays down specific exceptions for increasing the storage period of collected data. These exceptions include public interest, historical, scientific, and statistical reasons. The PDP Bill mandates the explicit consent of the data principal to store data for a longer duration of time than is needed to satisfy the purpose for which it is collected. The GDPR does not necessitate this consent.

SIGNZY

Next steps for PDP to become a Law

(1) Submission of the parliamentary committee report

(2) Passing by both houses of parliament, the Lok Sabha and the Rajya Sabha

(3) Presidential assent followed by notification in the official gazette

SIGNZY

References

[1] https://blog.signzy.com/data-privacy-the-debacle-the-debate-gdpr-vs-pdp-27691c9c2587

[2] https://prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf

[3] https://prsindia.org/billtrack/personal-data-protection-bill-2019

[4] https://www.cisomag.com/all-you-need-to-know-about-indias-first-data-protection-bill/

[5] https://economictimes.indiatimes.com/tech/internet/tech-companies-flag-licensing-non-personal-data-terms/articleshow/72500260.cms

[6] https://www.vantageasia.com/pdp-bill-reaches-parliament/

[7] https://indianexpress.com/article/explained/how-data-protection-bill-compares-with-its-eu-counterpart-6164237/

SIGNZY

For more information visit us at:

 : Signzy

 : signzy.com

 : @TeamSignzy

 : /TeamSignzy/

SIGNZY