India's Personal Data Protection Bill, 2019

(Tabled in the Lok Sabha on December 11 2019 and referred to a joint select committee of both Houses of Parliament)

The Personal Data Protection (PDP) Bill, 2019, which was initially introduced in 2018 by the B. N. Srikrishna committee, has undergone substantial changes since its introduction. The updated version of the bill has been made public and organisations across industries are evaluating the possible impact of the regulation on their businesses. While India-based organisations with global footprints have already taken measures to comply with regulations such as the European Union's General Data Protection Regulation (GDPR), entities which operate primarily in the Indian market are anxious to understand the impact of the bill on their day-to-day operations. We summarise the key highlights of the bill. The joint select committee will give its report before the end of the Budget Session 2020, which usually commences in the last week of January.

To be adopted by Will come into force on





Applicability

- Data fiduciary
- Data processor
- · Public company
- Private company
- Partnership firm
- Any other corporate body
- State entities (including government agencies)
- · Registered place of business within India

Fines of up to INR 15 crore or 4%

- · Offers goods or services to individuals in India
- Profiling of individuals in India

Penalties for non-compliance

of the organisation's total annual

3 years or a fine of

INR 2 lakh or both for re-

identification and processing

of de-identified personal data

for failure to comply with data

Penalty of up to INR 10 lakh

worldwide turnover

Imprisonment for

Types of data

Personal data is data about or relating to a natural person who is directly or indirectly

- contact details

Personal data

Can be stored outside India

Sensitive personal data

Transfer outside India if:

Critical personal data

To be processed only in India

certain exceptions, such as:

by Central Government.

Transfer outside India only under

To be stored in India

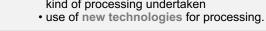
Government.

Sensitive personal data includes data such as:

- financial data/biometric data/genetic data
- health data
- · official identifier
- sex life/intersex status
- sexual orientation/transgender status
- caste or tribe/religious or political belief or affiliation
- any other data categorised as sensitive personal data by the authority under concerned sectoral regulators.

Critical personal

data: Categories of personal data to be notified by the Central Government in the future.



turnover

Government.

Social media intermediary may be classified as a significant data fiduciary by the Central

Data fiduciaries to be classified as significant data

volume and sensitivity of personal data processed

• risk of harm resulting from any processing or any

fiduciary by the Authority, based on:

kind of processing undertaken



Role of data fiduciaries The PDP Bill, 2019, details the functions of data

- fiduciaries, which incudes: · performing data protection impact assessment
- registering with the Authority
- maintaining records of data life cycle
- · conducting an independent annual audit of policies and processes.



Role of a consent manager

As per the PDP Bill, 2019, a consent manager:

- should enable a data principal to withdraw. review and manage consent through a platform
- must be registered with the Authority.



Exemption for government agencies

The PDP Bill, 2019, exempts government agencies from the proposed Act's applications in cases of:

- interest of sovereignty and integrity of India
- · security of the state
- · friendly relations with foreign states
- public order.

Privacy by Design (PbD)

The 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.

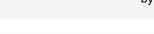


Child personal data

This provision in the bill necessitates verifying the age and obtaining the consent of a child's parent or guardian.

identifiable by:

- name
- address
- · educational details.



Transfer outside India permissible

· explicit consent has been obtained

· a contract or intra-group scheme exists

• permission has been given by the Central

• provision of health or emergency services

• where such transfer is deemed permissible



Data protection officer (DPO)

The PDP Bill, 2019, specifies certain rules for to the appointment of a DPO, such as:

- · allowing only significant data fiduciaries to appoint a DPO
- the DPO is to be based in India.



Processing by employer

Any personal data (excluding sensitive personal data) may be processed without consent if necessary for:

- recruitment or termination of employment
- provision of services/seeking benefits
- attendance verification
- performance management.



The Authority to make available a sandbox for innovation in artificial intelligence, machine learning or any other emerging technology.



Time frame within which days complaints made to the data fiduciary should be resolved.



Data principals have the right to erasure of their personal data that is no longer required for processing.

Key definitions

principal requests

- Data fiduciary is anyone who determines the purpose and means of processing of personal data.
- Data processor is anyone who processes personal data on behalf of a data fiduciary.
- Data principal is the natural person whose personal data is processed by a data fiduciary. • Authority is the Data Protection Authority, as formulated by the Central Government.
- · Social media intermediary is any entity who enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services.
- Consent manager is a data fiduciary registered with the Authority and enables a data principal to gain, withdraw, review and manage their consent.

