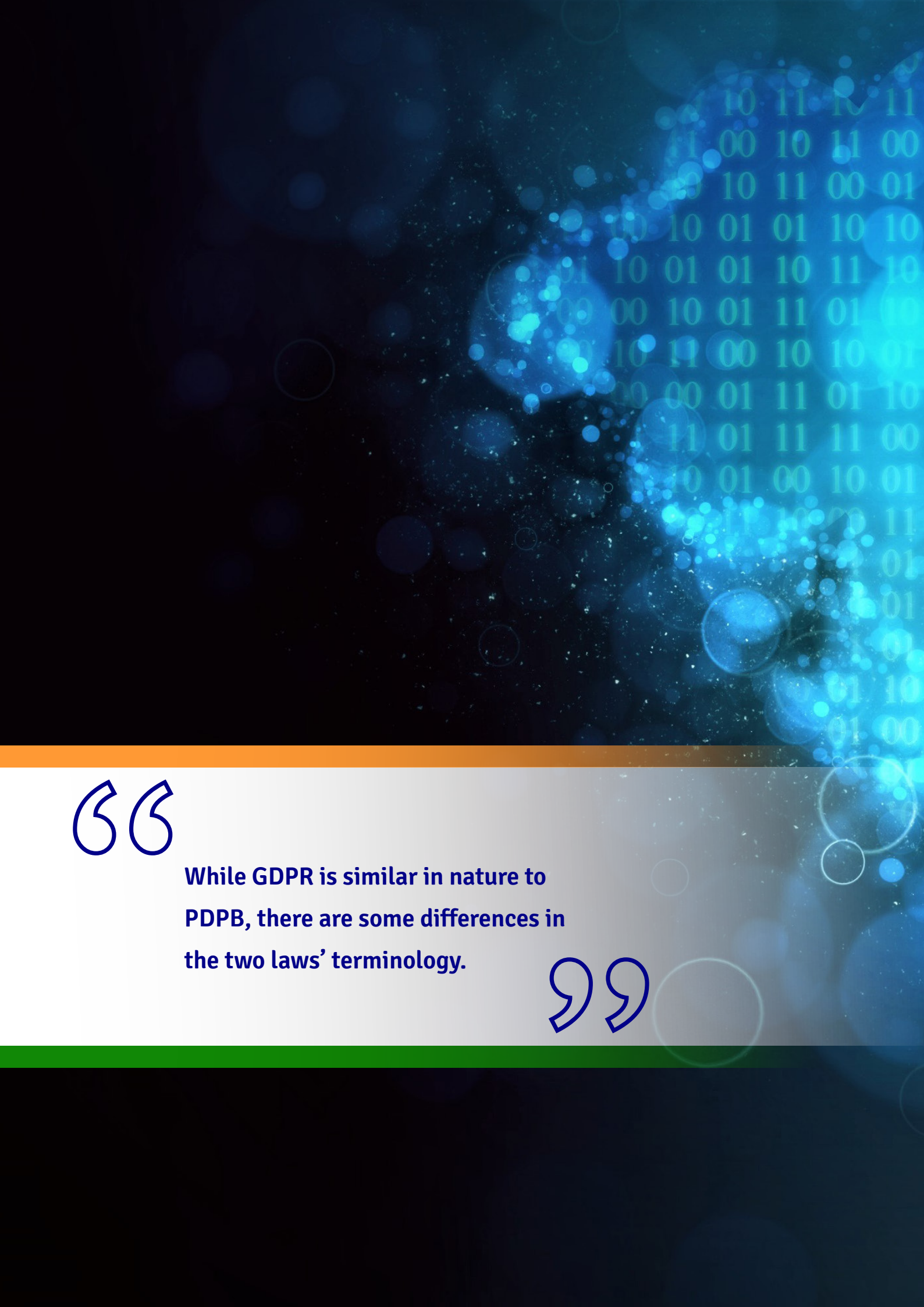
BigID

GUIDE TO

India's Personal Data Protection Bill (PDPB)

The Personal Data Protection Bill (PDPB) 2019, introduced into India's parliament on December 11, 2019, sets out to align India's data protection regime with the EU's General Data Protection Regulation (GDPR). The bill establishes protections on the cross-border flow of data and includes the creation of a Data Protection Authority (DPA).

Table of contents



While GDPR is similar in nature to PDPB, there are some differences in the two laws' terminology.

New Terminology Under PDPB

While GDPR is similar in nature to PDPB, there are some differences in the two laws' terminology. The term "data processor" is used in a similar manner, but instead of terms like "data controller" and "data subject," the law refers to "data fiduciary" and "data principal."

A **data fiduciary** is the entity who determines the purpose and means of processing the data.

A **data principle** is the natural person to whom the personal data relates.

Personal data is any characteristic, trait, attribute, or other feature that points to the identity of a natural person.

Sensitive personal data relates to financial data, health data, genetic and biometric data, caste, religious or political belief or affiliation, etc.

Sensitive personal data must be stored in India, but a copy of such data may be transferred outside of India in accordance with certain data transfer requirements such as explicit consent or when the DPA has specifically authorized the transfer.

Critical personal data — a unique and somewhat vague term under PDPB — is personal data that the central government determines to be critical personal data. The government is granted broad discretion to define critical personal data.

Critical personal data must be processed in India, except under emergency circumstances or where the government has approved the transfer, taking into account India's security and strategic interests.

Anonymized data is data that has undergone an irreversible process of transformation that makes it no longer identifiable to an individual.

Unlike GDPR, the central government and the DPA — the new regulatory body to be established by the central government — may direct a data fiduciary or data processor to disclose anonymized data or other non-personal data "to enable better targeting of delivery of services or formulation of evidence-based policies."

The Scope of PDPB

The scope of PDPB is potentially broader than that of the GDPR, as **it includes the processing of personal data by the state, any Indian company, any citizen of India, or any person or body of persons incorporated or created under Indian law.**

An entity may fall within scope merely by processing personal data in India — even through the use of a processor in India.

Records of Processing and Auditing

Unlike GDPR, which requires both data controllers and processors to maintain records of processing (except in narrow circumstances), PDPB requires only "significant" data fiduciaries to maintain records of processing activities.

The "significant" data fiduciary is determined by factors like:

- volume of personal data processed
- sensitivity of personal data processed
- turnover of the data fiduciary
- risk of harm by processing by the data fiduciary
- use of new technologies for processing, and additional factors

Data fiduciaries must retain records of processing that apply to "important operations" and periodically review security safeguards, Data Protection Impact Assessments (DPIAs), and other records that may be specified by regulations.

In addition, significant data fiduciaries are required to submit their processing for annual audit by independent auditors. Those data auditors may assign a "data trust score" to a data fiduciary based on their findings. This requirement more closely resembles mandates under the California Consumer Privacy Act.

Retention and Data Minimization

PDPB includes restrictions around data minimization, in which personal data must be **"collected only to the extent that is necessary for the purposes of processing of such personal data."**

PDPB also calls for specific storage limitations. Unlike GDPR, which permits retaining data in a form that no longer identifies an individual, PDPB requires deletion of that data unless the data fiduciary obtains consent from the data principal — or the data processing/retention is required by law.

Data fiduciaries are also required to conduct periodic reviews of whether personal data must be retained.

PDPB requires deletion of that data unless the data fiduciary obtains consent from the data principal — or the data processing/retention is required by law.

Data Rights

Like many comprehensive privacy proposals, the PDPB promotes consent based on data sharing, purpose limitation, and data minimization. Data principles receive certain rights similar to those covered by GDPR and CCPA, including:

The right to access	The requirement to provide the identities of all data fiduciaries with whom personal data has been shared could result in administrative burdens. It is not clear whether the "by any data fiduciary" language would also require documenting any onward transfers by data fiduciaries to whom personal data is disclosed.
The right to correction	This requires that companies correct, complete, or update personal data on request from the data principal. Companies may refuse a request if they disagree that the data is inaccurate, incomplete, or outdated — but must provide written justification for that decision and comply with a data principal's right to disclose their disagreement.
The right to data portability	The right to portability under the PDPB is broader than the corresponding GDPR right, as it is not limited to data that is processed under certain legal bases. The PDPB portability right also applies to profile information, even if the data may be inferred.
The right to erasure	This right ensures that a data principle must be able to seek erasure of their data being processed by a data fiduciary — including having it entirely deleted by a service provider.
The right to be forgotten	The PDPB distinguishes between the right to erasure and the right to be forgotten. The right to be forgotten involves the disclosure of personal data rather than its complete erasure. Unlike the GDPR, the PDPB places responsibility for determining the scope of application of the right to be forgotten on adjudicating officers appointed by the DPA, rather than on the controller.

Data Breach and Privacy Harms

The PDPB leaves it to the DPA to determine the deadline for breach notification — unlike the 72-hour rule under GDPR. The threshold for a reportable breach is higher under the PDPB, as it must be "likely" that the breach will cause harm to individuals.

The PDPB sets out a prescriptive list of what could constitute privacy harm, including:

- bodily or mental injury
- loss, distortion or theft of identity
- financial loss or loss of property
- loss of reputation or humiliation
- loss of employment
- any discriminatory treatment
- any subjection to blackmail or extortion
- any denial or withdrawal of a service, benefit, or good resulting from an evaluative decision about the data principal
- any restriction placed or suffered directly or indirectly on speech, movement, or any other action arising out of a fear of being observed or surveilled
- any observation or surveillance that is not reasonably expected by the data principal

The threshold for a reportable breach is higher under the PDPB, as it must be "likely" that the breach will cause harm to individuals.

Enforcement

The penalty provisions under both GDPR and PDPB are similar, with fines of up to 4% of global annual revenue.

The PDPB also includes criminal liability provisions. **Up to three years of imprisonment and a $3,000 fine is possible for someone who, knowingly or intentionally, re-identifies personal data that has been deidentified by a data fiduciary or processor without that entity's consent.**

PDPB Compliance Challenges

The PDPB presents a number of practical challenges for compliance. The first is the need for deeper data discovery. Traditional approaches to data discovery do not consistently identify personal and sensitive data for processing purposes.

An expanded definition of personal data, sensitive personal data, and critical personal data under PDPB requires that companies be able to automatically link and classify data — and understand how identifiers are related to each other based on measures like proximity.

In addition, the law's new data rights create a deeper need for businesses to understand data in context so they can appropriately process it, facilitate rectification and erasure requirements, and create policies in tandem with a strict set of legal bases for processing.

New retention requirements under PDPB create the need to set internal data retention policies that companies can act on immediately — including data collected via an online service — while also being able to identify duplicate and redundant data, which extends into the data governance space.

> **The PDPB presents a number of practical challenges for compliance.**

How to Achieve PDPB Compliance

Know your data: Combine the identification of personal data and the classification of sensitive data.

Understand whose data it is: Contextualize data with identity profiling and indexing that covers personal data and sensitive data.

Tag and label data for legal purposes: Ensure that data is being processed in accordance with defined legal bases of the law.

Minimize duplicate or sensitive data: Enable data minimization with duplicate identification and apply retention rules based on a disclosed purpose.

Manage data risk: Discover, classify, and map user credentials to apply controls for breach risk reduction.

Automate data access rights fulfillment: Automate manual fulfillment of individual data access and deletion requests.

Report on whose data you have: Enable correction workflows and validate whether sensitive data is being captured.

Detect out-of-policy, cross-border data transfers: Track data access, usage, and transfer violations across the organization for immediate action.

Looking Ahead

While PDPB raises some unanswered questions — including how much power the central government will have over citizens' data — **it presents the need for organizations to build and maintain flexible data frameworks.**

With a flexible framework that gives you full visibility into your data, your organization can ensure compliance with PDPB and keep up with the global trend toward stricter data protection.

See how BigID can help you ensure your organization's compliance with PDPB — now and in the future.

With a flexible framework that gives you full visibility into your data, your organization can ensure compliance with PDPB and keep up with the global trend toward stricter data protection.