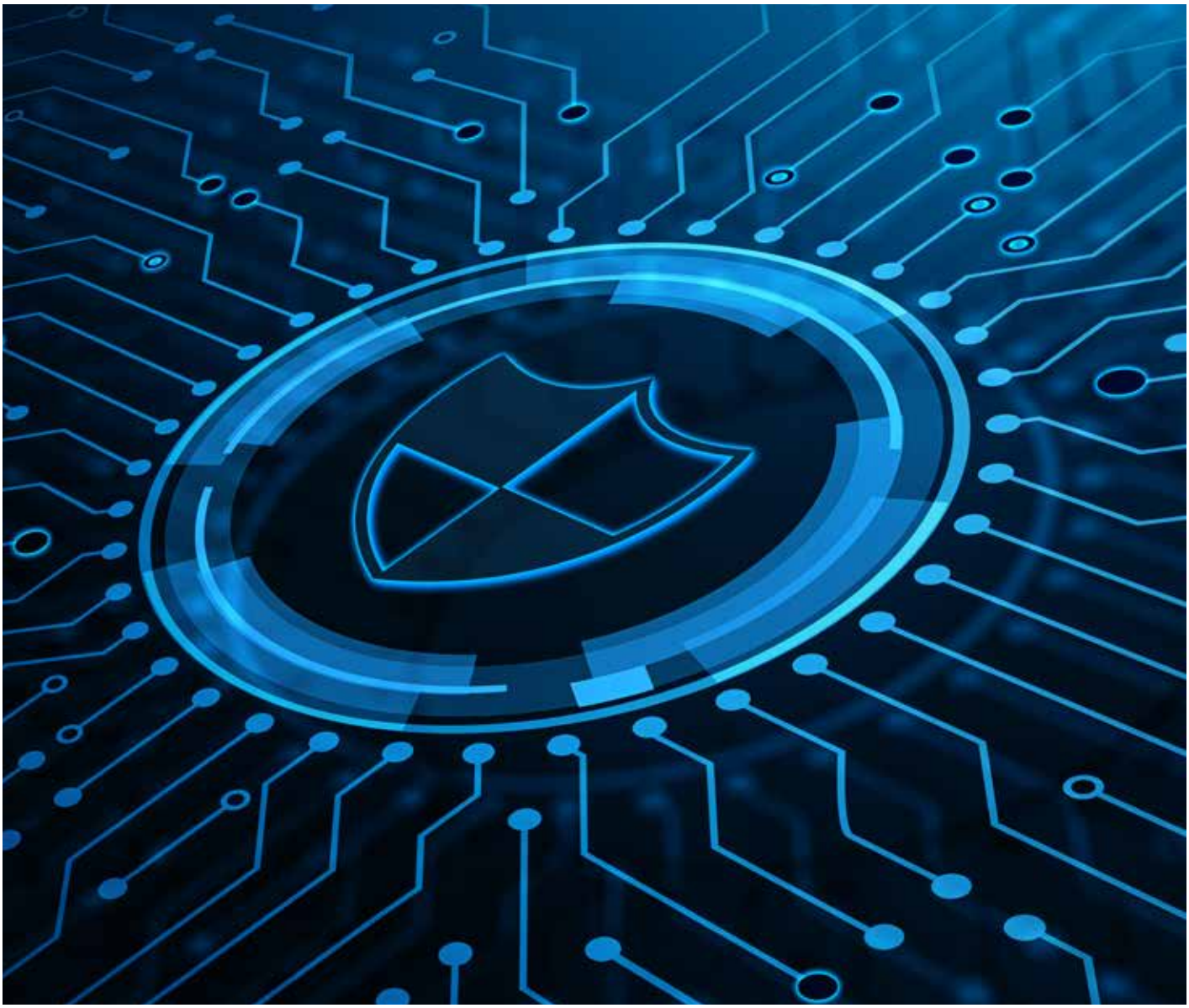
Deloitte.

The Digital Personal Data Protection Bill, 2023

Key provisions, enforcement, and implementation

August 2023

Table of contents



Introduction to the legislation

On 9 August 2023, the Digital Personal Data Protection Bill (DPDPB) of 2023, marking India's first comprehensive privacy law, was approved by both houses of the Parliament. The Bill has been designed to regulate the processing of digital personal data, acknowledging both individuals' right to safeguard their personal information and organisations' legitimate purposes for data processing. Once approved by a competent authority, it will be enacted as a regulation.

Enforcement timeline

The specific dates for enforcement of the Digital Personal Data Protection Bill, 2023, are currently awaiting final confirmation.

Key provisions of the Bill

Scope

The Bill defines personal data as any information that can directly or indirectly identify an individual. It encompasses the processing of personal data within India in digital format and digitized non-digital data. Additionally, the Bill applies to the processing of digital personal data beyond India if it pertains to offering goods or services to data principals within the country.

The Bill does not cover personal data processed by individuals for personal or domestic purposes or publicly available data.

Structure of the legislation

The Bill comprises 6 chapters, encompassing 33 sections and one schedule, detailing penalties for non-compliance.

Stakeholders

According to the Bill, "data principals" include individuals within India, as well as parents or lawful guardians of minors[1] and persons with disabilities. Additionally, the Bill defines the following key parties:

Agent of organisation or data processor: Any person processing personal data on behalf of a data fiduciary.

Appellate tribunal (Telecom Disputes Settlement): This tribunal handles appeals and complaints, related to orders or directions, issued by the Data Protection Board of India.

Consent managers: Individuals authorised by data principals to manage, review, and withdraw consent through an accessible, transparent, and interoperable platform, registered with the Board.

Data Protection Officer (DPO): An individual appointed by a significant data fiduciary to undertake activities assigned within the Bill.

Organisation or data fiduciary: "Person" (including organisations and associations) determining the purpose and means of processing personal data. Certain data fiduciaries may be categorised as "significant data fiduciary" based on the data they process.

Regulatory body - the Data Protection Board of India (DPBI/Board): The primary regulatory body responsible for enforcing the Bill.

Rights and obligations under the Bill

Data Principals

The Bill empowers individuals, i.e., data principals, with the following rights:

01 Receive information about their personal data.

02 Correct and delete their personal data.

03 Seek grievance redressal.

04 Nominate a third party to act on their behalf. Data principals are required to comply with applicable laws while exercising their rights under the Bill. Non-compliance may result in penalties of up to INR 10,000.

[1] Minor refers to an individual who has not yet completed eighteen years of age.

Data Fiduciary and Data Processor

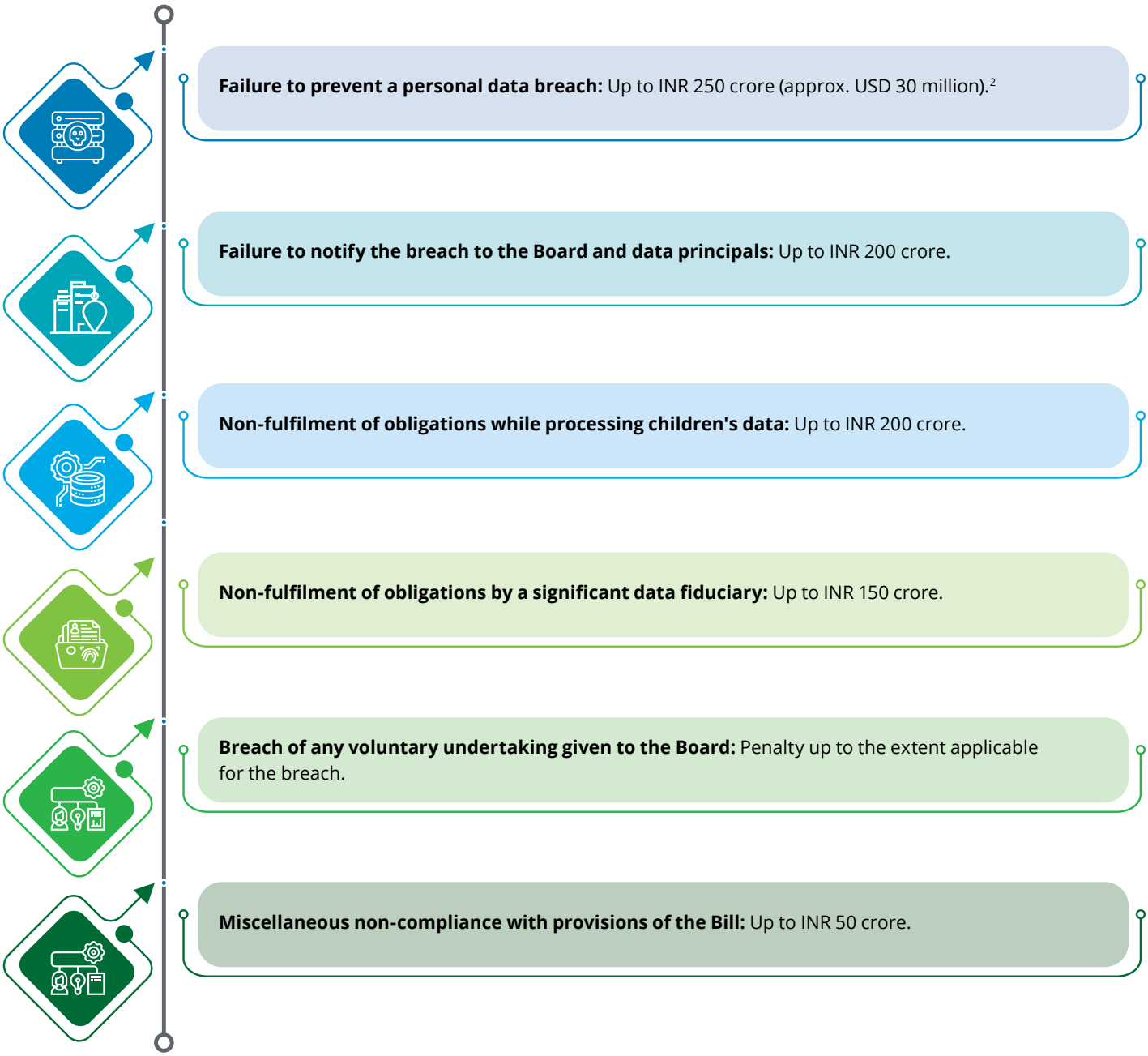
- **Compliance obligations:** Organisations must fulfil their responsibilities under the Bill, irrespective of agreements or non-compliance by data principals. They must ensure accurate and complete personal data for decision-making and disclosures, along with implementing adequate technical and organisational measures for compliance.
- **Notice:** Data principals should receive notices that specify the personal data processed, the purpose of processing, ways to exercise their rights, and contact information to reach the Board, for future data and for data that has already been captured before the enactment of the law. The notice should be provided in English or any of the 22 scheduled languages, depending on the data principal's preference.
- **Disclosures:** Data fiduciaries must provide details of all other data fiduciaries and data processors upon request by a data principal.
- **Consent:** Consent should be freely given, specific, informed, unambiguous, and followed up with clear affirmative action for a specified purpose.
- **Data handling:** Data fiduciaries should ensure accurate and complete processing of data, limiting it to specified purposes. Data must be erased once the purpose of processing is fulfilled, unless required for compliance with another law. Data fiduciaries may engage data processors only under valid contracts. The data of minors and persons with disabilities should be processed only with verifiable parental/guardian consent, and certain types of processing, such as tracking, behavioural monitoring, and targeted advertising directed at minors, are prohibited.
- **Breach notification:** In case of a data breach, the Board and affected data principals must be notified.
- **Significant data fiduciary:** Organisations falling under this category must appoint an India-based Data Protection Officer (DPO) and undertake additional measures such as Data Protection Impact Assessment and periodic data audits by an independent data auditor.

Transfer of personal data outside India

The Bill allows the free transfer of personal data outside India, except to countries expressly restricted by the Central Government. Furthermore, the Bill considers and retains provisions for other laws in India that may influence international data transfers.

Penalties for non-compliance

The Bill specifies various penalties for non-compliance, including:



- **Failure to prevent a personal data breach:** Up to INR 250 crore (approx. USD 30 million).[2]
- **Failure to notify the breach to the Board and data principals:** Up to INR 200 crore.
- **Non-fulfilment of obligations while processing children's data:** Up to INR 200 crore.
- **Non-fulfilment of obligations by a significant data fiduciary:** Up to INR 150 crore.
- **Breach of any voluntary undertaking given to the Board:** Penalty up to the extent applicable for the breach.
- **Miscellaneous non-compliance with provisions of the Bill:** Up to INR 50 crore.

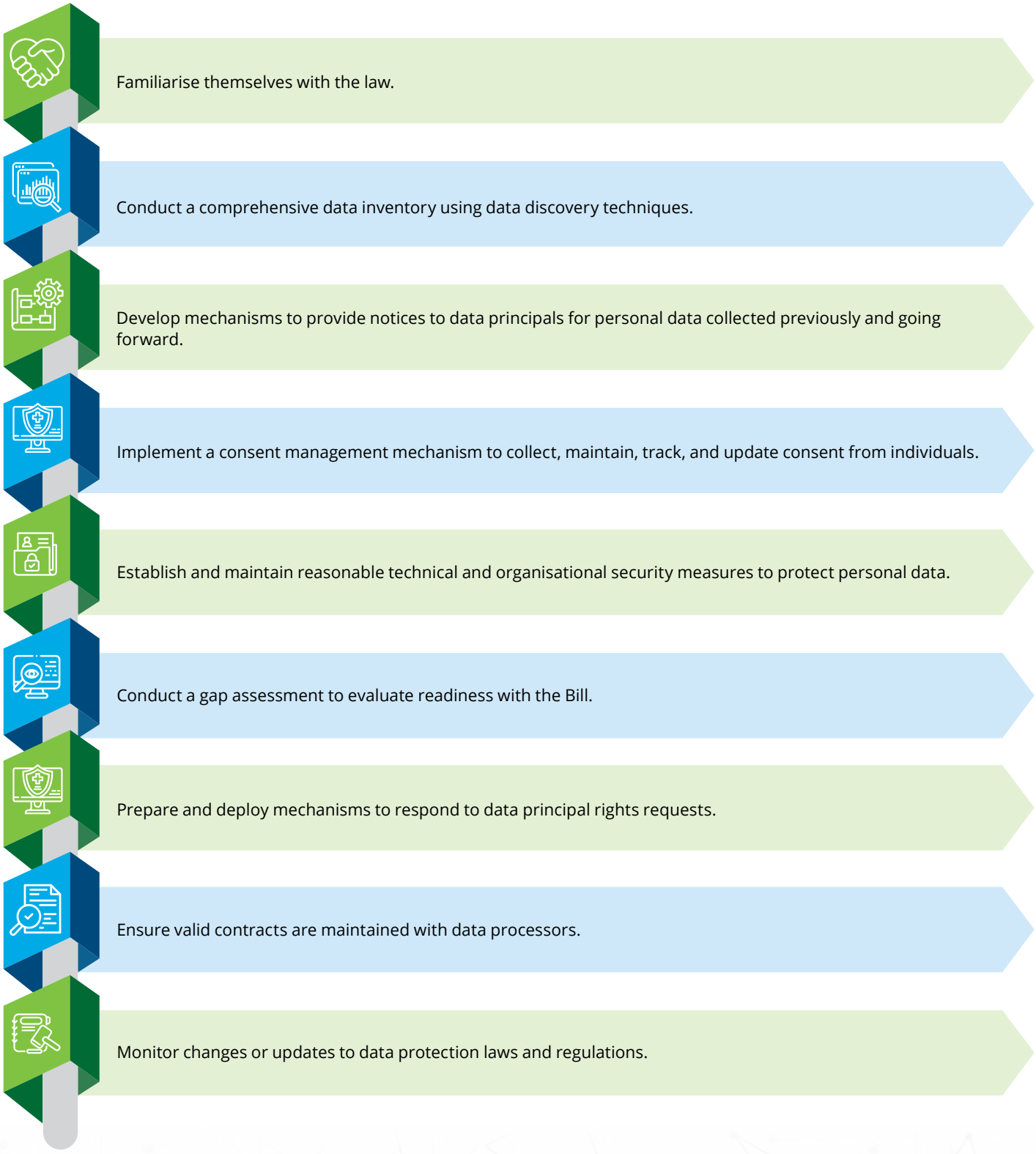
Enforcement and Governance

The Board, established by the Central Government, will be the statutory body responsible for enforcing the Bill. The Board's powers and functions include issuing guidelines and regulations, determining non-compliance, imposing penalties, issuing directions to remedy harm, and investigating violations.

[2] INR to USD conversion rate 1 USD = 82.13 INR

How can organisations prepare for compliance?

Organisations should take the following steps to prepare for the Bill:



Connect with us

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Abhijit Katkar
Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Tarun Kaura
Leader – Cyber Advisory, Risk Advisory
Deloitte India
tkaura@deloitte.com

Manish Sehgal
Partner, Risk Advisory
Deloitte India
masehgal@deloitte.com

Gaurav Khera
Partner, Risk Advisory
Deloitte India
gkhera@deloitte.com

Sowmya Vedarth
Partner, Risk Advisory
Deloitte India
sovedarth @deloitte.com

Deloitte.