



# Understanding the Digital Personal Data Protection Bill (DPDPB), 2022

A summary  
November 2022

# Table of contents

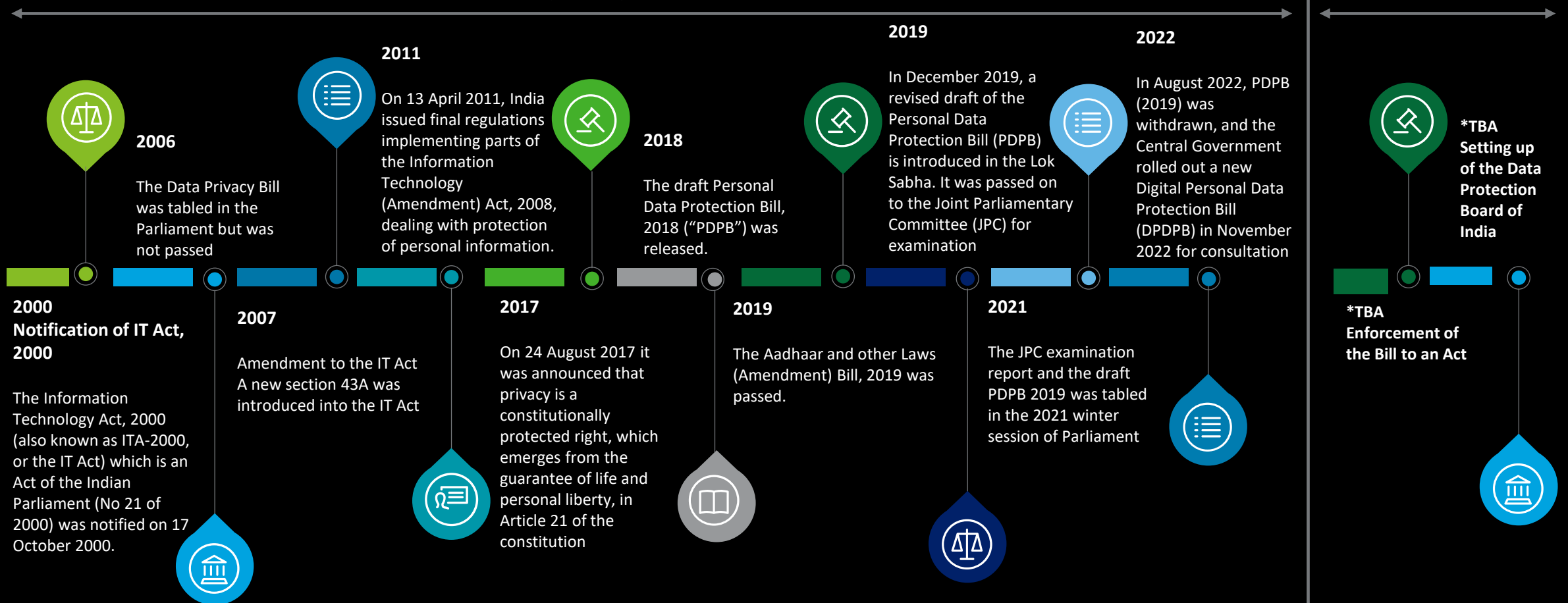
History of data privacy in India	3
Overview of the Bill	4
Introduction to the Bill	5
Applicability of the Bill	6
Key roles	7
Obligations under the Bill	8
The Privacy Notice, Consent Vs. Deemed Consent	9
Rights of Data Principal	10
Special Provisions: Transfer of personal data outside India	11
Special Provisions: Exemptions to the Bill	12
Penalties for Non-Compliance	13
Compliance framework	14
Way forward	15
Appendix: Key differences w.r.t GDPR, PDPB and DPDPB	16



# History of data privacy in India

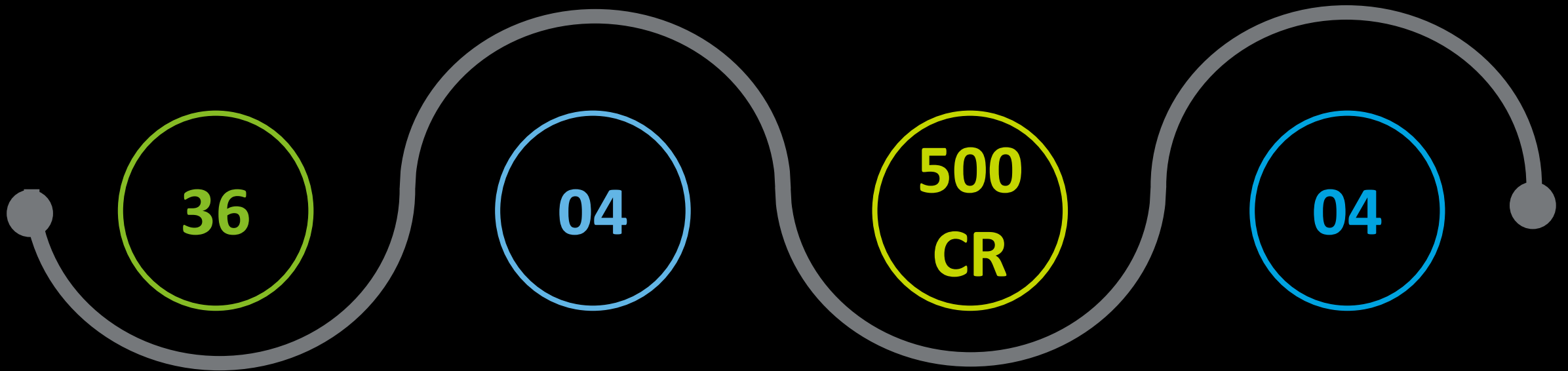
## The journey so far

## The journey ahead



\*TBA – To be announced

# Overview of the Bill



## CONTENTS

- 6 chapters
- 30 sections

## RIGHTS

- Right to information about personal data
- Right to correction and erasure of personal data
- Right of grievance redressal
- Right to nominate

## PENALTIES

- Maximum Penalty - not exceeding 500 crore per instance of violation
- Failure to prevent data breaches
  - Failure to notify data breaches
  - Non-fulfilment of additional obligations in relation to children
  - Non-fulfilment of significant Data Fiduciary obligation
  - Non-compliance with duties of Data Principal

## OBLIGATIONS

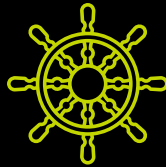
- Data Fiduciaries
- Significant Data Fiduciaries
- Data Processors
- Data Principals

# Introduction to the Bill

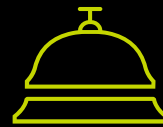
The Digital Personal Data Protection Bill (DPDPB), 2022 has been released with the scope of protecting the privacy rights and freedom of individuals in India. The Bill deliberates on the parties involved, governance, requirements, penalties, and grievance mechanisms to empower an individual and provide control over their personal data in digital format. Key parties defined under the bill are:



The individual i.e.,  
The Data Principal



Organisation i.e.,  
The Data Fiduciary



Agents of organisations  
i.e., The Data Processors



Regulatory body i.e.,  
Data Protection Board of India

## Coverage of the Digital Personal Data Protection Bill, 2022



Privacy Notices,  
Policies, and  
Procedures



Lawfulness  
and Consent  
Management



Data  
Principal  
Rights



Design and  
Implement Data  
Management



Technical and  
Security Controls



Grievance Mechanisms



Audit and Compliance




Governance  
and Penalties





# Obligations under the Bill

Following are the obligations for the different roles as per the DPDPB, 2022.

Data Fiduciary Chapter 2, Section 6 and 9	*Significant Data Fiduciary Chapter 2, Section 11	Data Processor Chapter 2, Section 9	Data Principal Chapter 3, Section 16	Significant Data Fiduciary 
<ul style="list-style-type: none"><li>• Lawful processing</li><li>• Notice and Consent</li><li>• Comply with the DPDPB</li><li>• Maintain accurate personal data</li><li>• Implement technical and security controls</li><li>• Data breach notification</li><li>• Data retention and disposal</li><li>• Publish business contact information of their Data Protection Officer</li><li>• Respond to Data Principal Rights requests</li><li>• Appoint a Data Processor under a valid contract</li><li>• Refrain from processing personal data that may cause harm to a child, or track them, and obtain parental consent before processing</li></ul>	<ul style="list-style-type: none"><li>• All obligations of the Data Fiduciary</li><li>• Appoint a Data Protection Officer</li><li>• Appoint an Independent Data Auditor</li><li>• Undertake Data Protection Impact Assessment</li><li>• Perform periodic Privacy based Audits</li></ul>	<ul style="list-style-type: none"><li>• To notify the Board and Data Principal in the event of a data breach</li><li>• To protect personal data in its possession</li><li>• To appoint another Data Processor under a valid contract, if permitted, in a contract with the Data Fiduciary.</li></ul>	<ul style="list-style-type: none"><li>• Do not register false complaints with Data Fiduciary or the Board</li><li>• Do not furnish false or suppress material information</li><li>• Furnish authentic and verified information for Data Correction and Erasure requests</li></ul>	<p><b>*The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, based on an assessment of relevant factors</b></p> <ul style="list-style-type: none"><li>• Volume and sensitivity of personal data processed</li><li>• Risk of harm to the Data Principal</li><li>• Security of the state</li><li>• Public order</li><li>• Potential impact on the sovereignty and integrity of India</li><li>• Risk to electoral democracy</li><li>• Such other factors, as it may consider necessary</li></ul>



# The Privacy Notice, Consent Vs. Deemed Consent

The bill has defined 'Consent' in a very clear language as the freely given, specific, informed, and unambiguous indication of the Data Principal's wishes through an affirmative action.

## Key features of the Notice



An itemised notice is required to be presented to the Data Principal by the Data Fiduciaries at the time or before collecting the personal data and it must provide a description of what personal data is collected and for what purpose.



The notice has a retrospective effect which means that for the personal data collected before the rollout of the bill, Data Fiduciaries shall provide an itemised notice to the Data Principal and describe what personal data has been collected and the purpose of processing, as soon as it is reasonably practicable.

## Key features of Consent



It is imperative for the Data Fiduciaries to raise a request for consent in plain and clear language with the contact details of the DPO.



The bill has also focussed on the right to withdraw consent and the ease of withdrawal. It shall not affect the lawfulness of the processing.



The bill has made room for a 'Consent Manager' as a registered entity to give, manage, review, and withdraw consents on behalf of the Data Principals.

## Deemed Consent

Consent is considered deemed in the following cases of processing:



For voluntarily provided personal data with reasonable expectation



For performance of any function under the law



For medical emergencies involving vital interest or public health



For taking measures to ensure safety and public order



For certain purposes related to employment



For activities in public interest

# Rights of Data Principal

Under the DPDPB, 2022 the Data Principal has the following rights as enumerated in Chapter 3 of the Bill:

## Right to information about personal data (Section 12)

Data principal has the right to obtain confirmation on the processing of data, summary of the personal data being processed and identities of all data fiduciaries processing the data.

## Right to nominate (Section 15)

In the event of death or incapacity a Data Principal shall have the right to nominate any other individual to exercise the rights of data principal.



## Right to Grievance Redressal (Section 14)

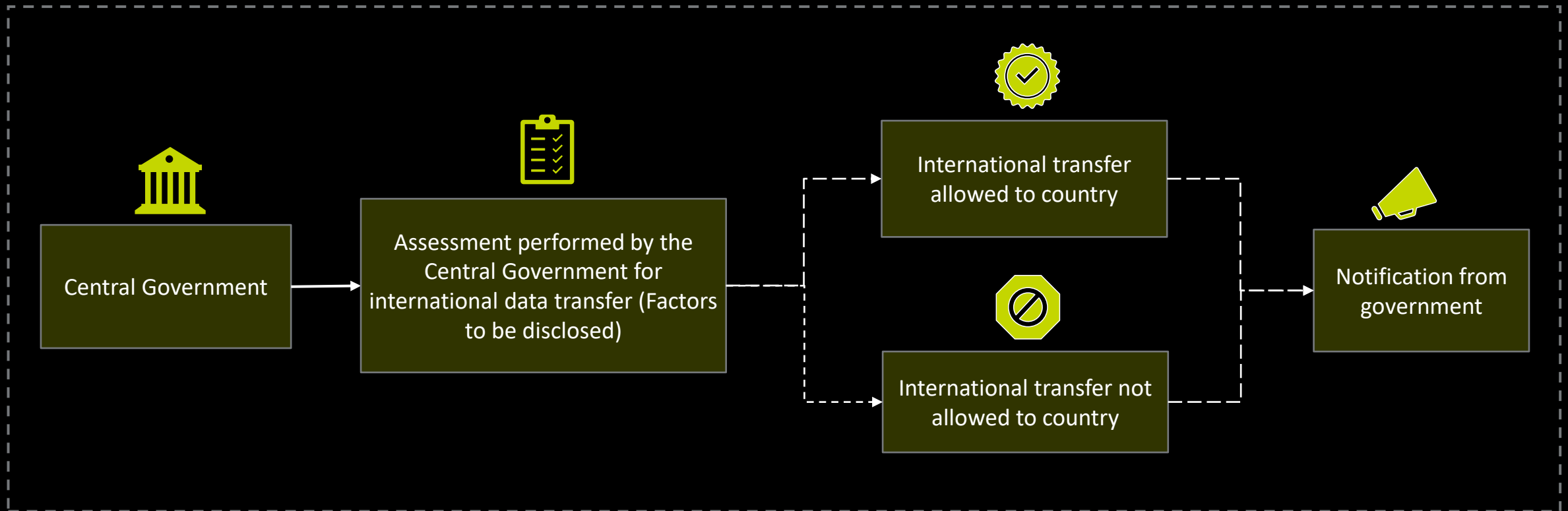
A Data principal shall have the right to register a grievance with the data fiduciary. If the data principal is not satisfied or does not receive a response within 7 days from data fiduciary, then he may register a complain with the board in such manner as may be prescribed.

## Right to correction and erasure (Section 13)

Data Principal shall have the right to correction and erasure of personal information, which includes correction, completion, or updating of personal data.

# Special provisions: Transfer of personal data outside India

As Per Section 17 of the DPDPB 2022, the Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data in accordance with provisions of the act in the manner enumerated below:



# Special provisions: Exemptions to the Bill

Following are the exemptions enumerated in Chapter 4 (Section 18) of DPDPB 2022, for the processing of personal data. They are spread across 3 categories:

## General Exemptions

As per Section 18(1), the following personal data processing activities are exempted where it is necessary:

- For enforcing legal rights and claims
- For court and legal proceedings
- For law enforcement and investigation
- For processing personal data of Data Principals for a contract outside India

### Exempted obligations under Section 18(1)

All obligations of Data Fiduciary under:

- **Chapter 2 except Section 9(4)** - Reasonable security safeguards to prevent a personal data breach.
- **Chapter 3:** Data Principal Rights and Duties
- **Section 17:** Transfer of personal data outside India

## Special Exemptions

As per Section 18(3), the Central Government may exempt certain Data Fiduciaries or class of Data Fiduciaries on the basis of:

- Volume of personal data processed
- Nature of personal data processed

### Exempted obligations under Section 18(3)

- **Section 6:** Notice
- **Section 9(2),(6):** Data Accuracy, Retention and Disposal
- **Section 10:** Processing of Children's Personal Data
- **Section 11:** Additional obligation of Significant Data Fiduciary
- **Section 12:** Right to information about personal data

## Exemptions for Central Government and States

As per Section 18(2), The Central Government may, by notification, exempt from the application of provisions of this Act, the processing of personal data:

- by any instrumentality of the State in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, and public order
- Necessary for research, archival, and statistical reasons where no decision will be taken specific to the data principal

As per Section 18(4), Section 9(6) of the Bill shall not apply in respect of Personal Data processing by States or any instrumentalities of the States

**Section 9(6):** Data Retention and Disposal

# Penalties for non-compliance

Several Penalties fall under the ambit of DPDPB, 2022 to enforce the requirements of the Bill and secure the rights and freedom of Data Principals as enumerated in Schedule 1 of the Bill. Further to note, as per Section 25(1), the maximum fine in each instance shall not exceed 500 crore rupees. The fines are listed as follows:



- 1. Penalty for Failure to protect a data breach –** INR 250 Crore. Additionally, the bill has introduced a penalty of INR 500 crore in case of significant non-compliance.



- 2. Notification to Board and Data Principals-** Failure to notify the Board and Data Principals in case of a data breach – INR 200 crore



- 3. Children's data -** Non-fulfilment of obligations while processing children's data - INR 200 crore

- 4. Significant Data Fiduciary -** Non-fulfilment of obligations when the government notifies a Significant Data Fiduciary - INR 150 crore



- 5. Non - Compliance of duties of Data Principal –** INR 10,000



- 6. Miscellaneous -** Non-compliance with provisions of this Act other than those listed in (1) to (5) - Penalty up to INR 50 crore



# Highlights of the Data Protection Board of India

The bill establishes a Data Protection Board of India to ensure compliance. The composition of the board and its establishment procedure shall be determined by the central government.

## Functions of the Board



To receive complaints and pronounce decisions



To determine non-compliance and impose penalties



To allocate work and form groups for hearing



To issue directions for hearing and modify, suspend, withdraw, or cancel them.



To direct the Data Fiduciaries to adopt certain measures in case of a data breach

## Alternate Dispute Resolution



The Board may direct the parties for alternate dispute resolution where it deems fit.

## Review and Appeal



The Board may review its order for reasons to be recorded in writing.



An appeal against the order of the Board shall lie with the High Court within a period of 60 days.

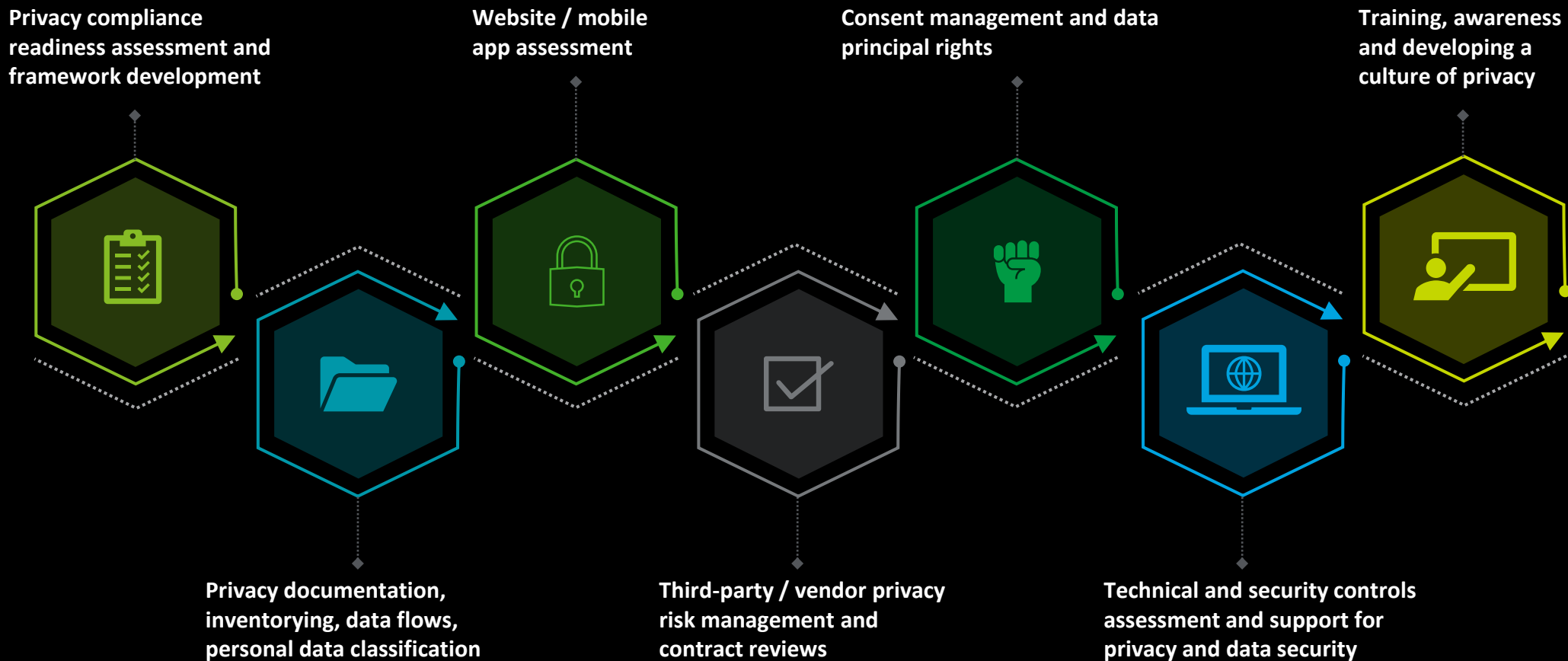
## Voluntary Undertaking



The Board may accept a voluntary undertaking regarding compliance from any person at any stage

# Way forward for Compliance and Readiness

What's next? Data Fiduciaries and Processors may leverage Deloitte's expertise in the journey towards compliance. A wide range of Data Privacy offerings based on tried and tested methodologies are available to handhold and ensure a smooth transition to a pro-privacy operating model.



## Appendix: Key differences regarding GDPR, PDPB, and DPDPB

Features and requirements	General Data Protection Regulation, 2018	Personal Data Protection Bill, 2019	Digital Personal Data Protection Bill, 2022
Implied/Deemed Consent	✓	✗	✓
Records of processing activities	✓	✓	✗
Data flow diagrams	✓	✓	✗
Data localisation	✗	✓	✗
Cross-border data transfer requirements	✓	✗	✓
Special categories of personal data	✓	✓	✗
Significant categories of Data Controllers/Fiduciaries	✗	✓	✓
Right to data portability	✓	✓	✗
Right to nominate	✗	✗	✓
Responsibilities and penalties for data subject/principal	✗	✗	✓
Data breach timelines	✓	✗	✗
Data principal rights response time	✓	✓	✗





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.

© 2022 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited