KPMG

Digital Personal Data Protection Bill

A perspective on India data protection regime

December 2022

Introduction:

In the month of August, The Ministry of Electronics, and Information Technology (Government of India) had withdrawn Personal Data Protection Bill 2019 owing to multiple recommendations received through public consultation. As revised version of its predecessor, the Government released Digital Personal Data Protection Bill on November 18. This Bill is a part of a list of legislations that includes IT rules, National Data Governance Framework Policy and a new Digital India Act.

Key Highlights of the Bill

1. The scope of the Bill is limited to personal data which is collected online or personal data that is collected offline and subsequently digitized.

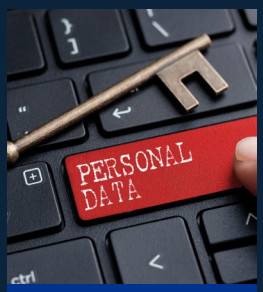
2. The Bill has introduced certain duties for Data Principals to ensure that rights provided to Data Principals are not misused. The Bill also imposes a penalty up to INR10,000 for breach of duty.

3. The Bill has introduced the provision of Voluntary Undertaking which would allow organisations to furnish undertakings if they are unable to comply with the provisions of the Bill. This would allow the organisations to avoid penalty proceedings.

4. The Bill mandates that request for consent and the notice given to Data Principal shall be accessible in English or any other language (22 languages) included in Eighth Schedule to the Constitution of India, at the option of the Data Principal.

5. The Bill has entirely omitted any kind of criminal penalty for non-compliance with the provisions of the Bill. The Bill imposes financial penalties up to INR500 crores per instance.

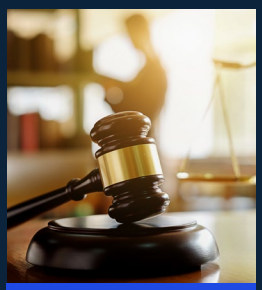
How different is DPDPB 2022 from its predecessor



Scope and Applicability

PDPB 2019:
- Personal data collected, disclosed, shared or processed within the territory of India.
- Organisation not present in India, but process personal data related to offering goods and services or profiling individuals in India.

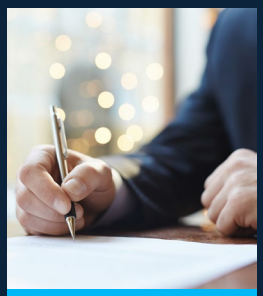
DPDPB 2022:
- Processing of digital personal data within the territory of India where personal data is collected online and such personal data is digitised
- Processing is related to offering goods and services or profiling.



Lawful Basis of Processing

PDPB 2019:
- Consent,
- Legal obligation
- Vital interest
- Public interest
- Performance of Contract, legitimate interest

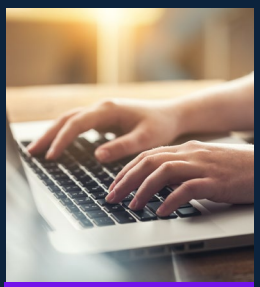
DPDPB 2022:
- Consent
- Deemed consent



Consent

PDPB 2019:
Clear , specific and informed and being capable of withdrawn

DPDPB 2022:
Explicit consent and Deemed consent



Registration

PDPB 2019:
Significant Data Fiduciaries are required to register with the Data Protection Authority

DPDPB 2022:
Consent Manger to register with the Data Protection Board

Appointment of DPO

PDPB 2019:
Mandatory for Significant Data Fiduciaries and the DPO should be based in India

DPDPB 2022:
Mandatory for Significant Data Fiduciaries

Breach Notification

PDPB 2019:
Data Fiduciary must notify the Data Protection Authority as soon as possible and publish on its website as directed by the Data Protection Board

DPDPB 2022:
Data Fiduciary or Data Processor to Data Protection Board and each affected Data Principal

Data Subject Rights

PDPB 2019:
Right to Access
Right to Data Portability
Right to Correct
Right to be Forgotten

DPDPB 2022:
Right to obtain Information
Right to Correction and Erasure/Forget
Right of Grievance Redressal
Right to Nominate

Cross Border Data Transfer

PDPB 2019:
Sensitive personal data must be stored in India but may be transferred outside India where:

- Data Principal has provided consent
- Pursuant to contract or intra group scheme
- Data Protection Authority has approved the transfer

DPDPB 2022:
Central Government will provide a list of countries to which personal data can be transferred

Penalties

PDPB 2019:
Administrative fines up to the higher of approximately INR15 crore or a 4% of group annual turnover
Criminal liability up to three years imprisonment

DPDPB 2022:
Data Principal: up to INR10,000 and Data Fiduciaries up to INR500 crores for each instance

A perspective on the Bill

Applicability of the Bill:

While the Bill applies to processing of digital personal data within India and processing related to offering goods and services and profiling of Data Principals within India, it does not highlight whether it would apply to any individual whose personal data is processed within the territory of India.

Sensitive Personal Data:

The Bill does not differentiate between personal data and sensitive personal data. The bill has taken a holistic approach of safeguarding all personal data with equal level of protection as it mentions obtaining explicit consent for collection of personal data.

Privacy notice:

- ***Elements of Privacy Notice***: The Bill requires Data Fiduciaries to provide Data Principals with a notice stating the personal data collected and the purpose of processing. The Bill should also consider inclusion of elements such as details of Data Fiduciary, information about the third parties with whom the personal data has been shared with, and any other such information that would help the Data Principal to make an informed decision.
- ***Retrospective Application***: The provision of providing notice to the data principals have retrospective application where the Data Fiduciary is required to provide the itemised notice to the Data Principal who has given her consent prior to commencement of the Bill within reasonable time. This retrospective application would be challenging for Data Fiduciaries who had processed personal data based on consent of the Data Principal.

Non-automated means:

The provisions of the Bill do not apply to non-automated processing of personal data. This could lead to exclusion of number of Data Fiduciaries who do not carry out processing of personal data by automated means. To include such Data Fiduciaries in the scope of the Bill, the Bill should consider application of provisions on processing of personal data by partially automated means and to processing other than automated means.

A perspective on the Bill

Breach notification:

- In the event of a data breach, the Bill imposes an obligation on Data Fiduciary and Processor to notify each affected Data Principal. This is a welcome move since the Data Principals whose personal data has been compromised would be informed about all kinds of data breaches irrespective of the severity of risk to them.
- The Bill does not specify any particular time period in which the Data Fiduciary is required to inform the Data Protection Board and Data Principals regarding data breach.

Privacy by design and default:

The Bill does not contain provision regarding privacy by design and default. This could weaken the overall privacy centric approach to be adopted by Data Fiduciaries while developing new systems and applications. The Bill should consider imposing an obligation on Data Fiduciaries to implement Privacy by design and default in all their practices and technical systems.

Rights of Data Principal:

Right to grievance redressal: The Bill has introduced right to grievance redressal where the Data Fiduciary is required to respond to the grievance of Data Principal within 7 days or shorter period that may be prescribed. This is a welcome move to reduce the time taken by Data Fiduciary to acknowledge the grievance of the Data Principal and provide appropriate solution for the same.

Right to data portability: The Bill does not provide the right to data portability to Data Principal. In this era of population-scale data silos, individuals should be able to extract data related to them from data silos in which they have been stored. A right to data portability will not only give individuals more meaningful control over their data, it also will serve as an effective measure to prevent the consolidation of data in the hands of few.

Right to access: The Bill provides the Data Principal with right to obtain information regarding the categories of personal data shared and identities of all the Data Fiduciaries with whom the personal data has been shared. This right should be extended to include the right to obtain information about Data Processors with whom the personal data has been shared.

Right to nominate: The Bill has introduced a unique right to nominate a representative in case of incapacity or death of the Data Principal to exercise their right. This could provide adequate guidance to certain sectors facing such scenarios and ensure protection to Data Principal whose data is being processed in line to the processing activities.

A perspective on the Bill

Cross border data transfer:

The Bill has eased the cross-border data transfer requirement where the Data Fiduciaries can transfer the personal data to other countries that are notified by the Central Government. Further, eliminated the requirement to store sensitive personal data within India. This came as a big relief for the Data Fiduciaries who maintain their servers in foreign nations and startups who will not be compelled to invest in local storage solutions. However, the Bill can consider coming up with a legal mechanism to transfer the personal data to countries which are not included in the whitelist of Central Government.

Personal data of children:

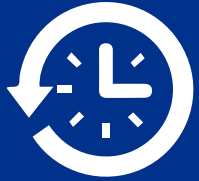
- The Bill prohibits tracking or behavioural monitoring of children and targeted advertising directed at children. Although this is the right step towards protecting the interest of minors, it could force major edtech and gaming organisations that cater to children to revisit their business model and marketing strategy.
- The provision of the Bill mandates obtaining verifiable parental consent before processing personal data of children. However, further clarity is required as to what would constitute as a verifiable consent.

Deemed consent:

The Bill allows processing of personal data on the basis of deemed consent. Under deemed consent, a bundle of different basis of processing such as legal obligation, contractual obligation, vital interest, public interest, legitimate interest has been included. Bundling of these different basis of processing under the umbrella of deemed consent would mean that the data principal may withdraw her consent which could affect the processing of personal data. The Bill should come up with other categories of lawful basis of processing which would be independent of consent.

Implementation timeline:

The Bill does not specify the implementation timeline however this would obligate the organisations to adopt a more proactive approach in complying with the provisions of the Bill.

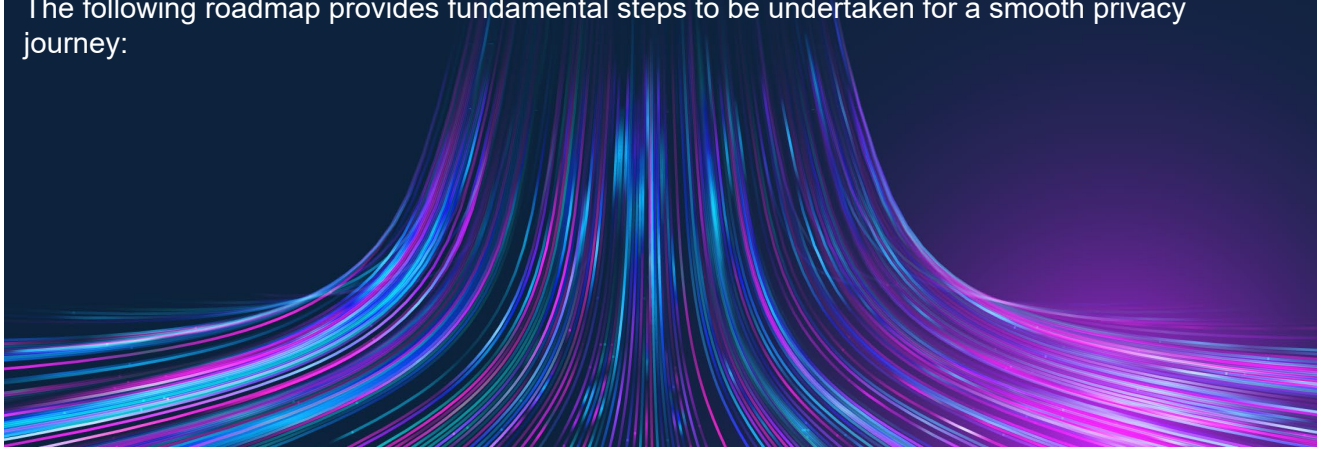


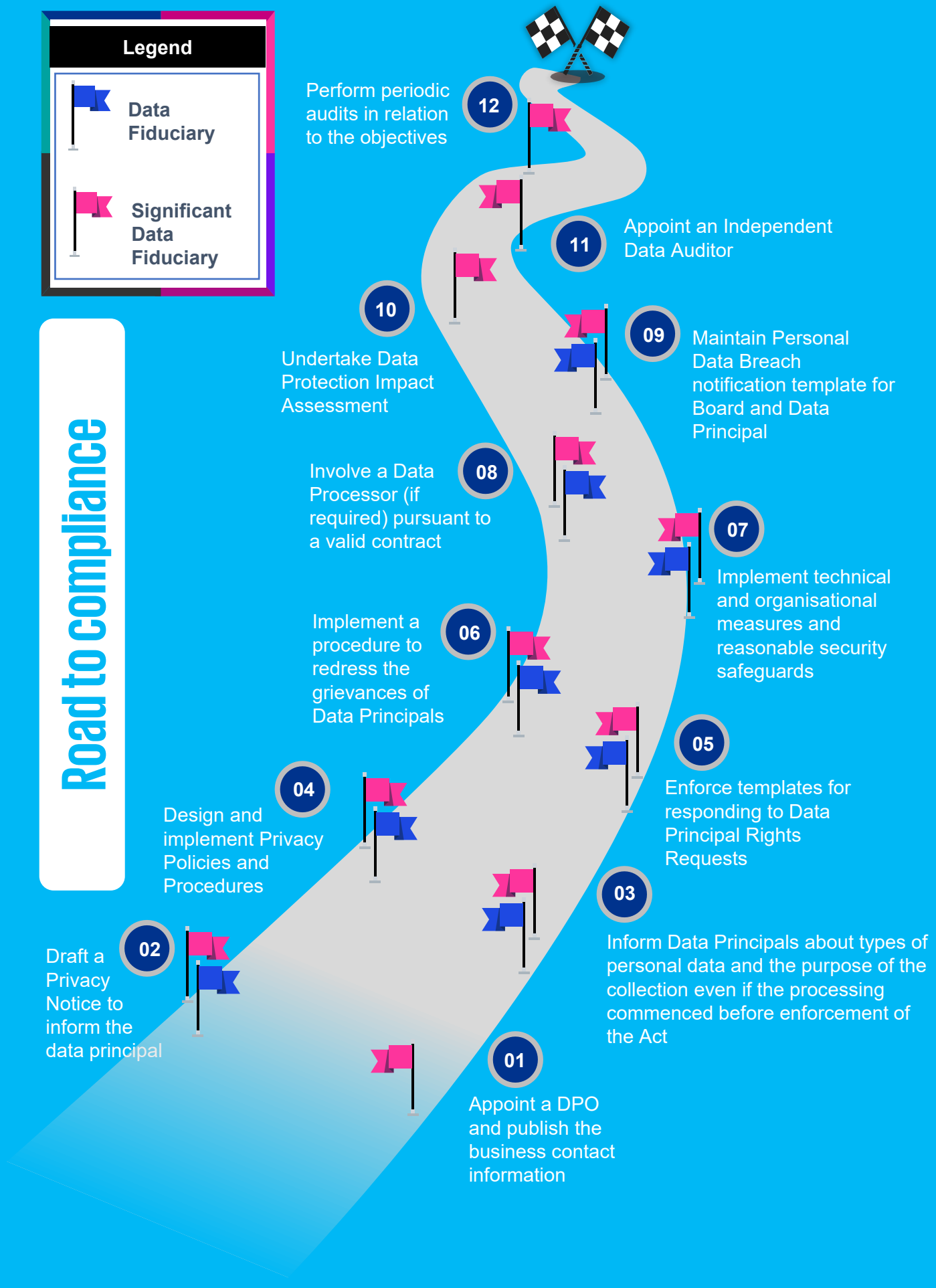
Potential impact on Industries

- India's Data Protection regime has taken a step ahead towards digitisation by introducing this Bill. It has adopted a liberal approach to strengthen India’s ability to attract foreign investments, support startup ecosystem and reduce compliance burden for organisations of different scale and size. However, it remains to be seen on how the Central Government addresses certain open-ended requirements in the Bill which could play an important role in determining the future of data protection.
- The Government has decided to take a phased approach in addressing the need for a data protection regime in India by releasing an initial bill, which could be followed by supplementary rules and guidelines. The phrases such as “as may be prescribed” are sufficient to understand that there is certainly more fuel left in the tank.
- Large scale, consumer centric organisations, which include but not limited to technology, telecommunication, healthcare, banking and financial and e-commerce that process personal data in large scale are likely to encounter stringent obligations than others due to parameters such as volume and sensitivity of personal data being explicitly highlighted in the bill.
- Organisations leveraging or focused on emerging technologies, such as Virtual Reality, Artificial Intelligence, Internet of Things (IoT), Robotic Process Automation (RPA), Web 3.0 and Metaverse to name a few, process and generate large volumes of personal data. This bill will encourage innovation and enable such organisations to consume and handle personal data with adequate safeguards in an ethical manner.
- The Bill has remodeled the approach of cross border data transfer which plays a crucial role in easing data flows for MNC’s. The Bill has excluded data localisation requirements which will help in enabling small, medium and large enterprises to store data across geographies resulting in reduction of costs and time spent on localised data storage.
- The Bill provides greater emphasis and encourages organisations to digitise personal data. Presently, the cost of collecting and managing offline data in physical form is much higher and unsustainable as compared to data in digital form. Additionally, the consumers would favour organisations handling the personal data in digital format because it would fall under the purview of this Bill, and it would be adequately protected. However, it would be interesting to understand the decisions undertaken by small scale organisations and family run businesses.

What should organisations do to meet the requirements of DPDPB 2022?

As a way forward, organisations need to be proactive and start working towards getting compliant with the regulatory obligations highlighted by the Bill rather than waiting for it to come into effect. The following roadmap provides fundamental steps to be undertaken for a smooth privacy journey:





Acknowledgements:

We are extremely grateful to senior leaders from the industry, subject matter experts, and KPMG in India team members for extending their knowledge and insights to develop this document.

Authors

- Rupak Nagarajan
- Nakuleesh Sharma
- JCS Karthik
- Prashant Kshirsagar
- Ayush Patel
- Anushka Singh
- Swetha Krishnan
- Mira Subramanian

Design, compliance and support

- Darshini Shah
- Sameer Hattangadi

KPMG in India contacts:

Atul Gupta
Partner and Head Digital Trust
Mobile: +919810081050
E: atulgupta@kpmg.com

Mayuran Palanisamy
Partner, National Lead, Data Privacy
Mobile: +919600057046
E: mpalanisamy@kpmg.com

Nitin Shah
Partner and Lead Cyber Strategy and Governance
Mobile: +919560244888
E: nitinshah@kpmg.com

Jignesh Oza
Partner, Digital Trust
Mobile: +919967545665
E: joza@kpmg.com

home.kpmg/in

home.kpmg/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

Printed in India.