KPMG

Decoding the Digital Personal Data Protection Act, 2023

August 2023

kpmg.com/in

The Digital Personal Data Protection Act 2023 (DPDPA)

The DPDPA 2023 is the onset of the data protection regime in India. It emphasises and encourages organisations to protect digital personal data while safeguarding the freedom of individuals.

Journey until now

2017
Supreme Court affirms privacy as fundamental right

2018
Draft Data Protection Bill

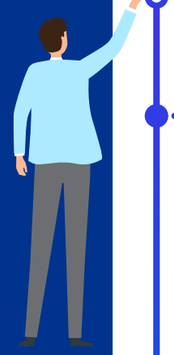
2019
Introduction of the Personal Data Protection Bill (PDPB)

2021
Parliamentary Committee report on PDPB

2022
Withdrawal of PDPB, 2019 and release of draft Digital Personal Data Protection Bill

2023 - July
- Cabinet approval of the DPDP Bill

2023 - August
- 'DPDP Bill, 2023' was passed by both houses of the Parliament and received Presidential assent and notified in gazette to become an enforceable Act



Territorial Scope

- Processing within the territory of India
- Processing outside India in connection with any activity related to offering goods and services within India

Material Scope

- Personal data that is collected in digitised form
- Personal data that is collected in non- digital form and digitised subsequently.

Rights of Data Principals

Right to grievance redressal
The Data Fiduciary and Consent Manager is required to respond to the grievance of the Data Principal within a time period as may be prescribed

Right to nominate
Data Principals have the right to nominate any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal

Right to access information about personal data
The Data Principal can exercise their right to obtain confirmation from the Data Fiduciary regarding data processing, summary of personal data and identities of all Data Fiduciaries and Data Processors

Right to correction and erasure of personal data
Data Principal can reach out to Data Fiduciary in order to exercise their right to correct, complete, update and erasure of their personal data

There are two grounds of processing defined in DPDPA under which organisations can process personal data:

Consent

The Data Principal may **give, manage, review, or withdraw their consent** to the Data Fiduciary directly or through a Consent Manager. Privacy notice to be provided at the time of obtaining consent.

Consent should be

01 Freely given
02 Specific
03 Informed
04 Unconditional
05 Unambigious
06 Requires affirmative action

FAQ

Q. Who will provide consent?
A. Data Principal

Q. Who will ask for consent?
A. Data Fiduciary

Q. How consent should be requested?
A. • In clear and plain language
• Using itemised notice

Q. How can consent be withdrawn?
A. By contacting Data Fiduciary or Consent Manager

Certain Legitimate Uses

No separate consent is required for certain "legitimate uses" recognised under the Act. This includes where data is **voluntarily** provided or collected for a **legal obligation.** Privacy notice is not required for legitimate uses.

Scenarios covered under Legitimate Uses

- For personal data provided **voluntarily** by the Data Principal
- For personal data processed for any function under **any law or judgement issued under law**
- For responding to a **medical emergency** involving a threat to the life of the Data Principal or other individual
- For maintaining **public order and ensuring safety**
- For purposes related to **employment**
- For performing activities in **public interest**

Table of Contents

1. Introduction

The first draft of the Data Protection Bill came out in 2018. After various rounds of amendment in 2019 and 2021, the bill was scrapped and replaced with the Digital Personal Data Protection Bill, 2022. The Digital Personal Data Protection Bill, 2023 introduced on 3 August 2023 and was passed by the Lower House of the Parliament on 7 August 2023 and by the Upper House of the Parliament on 9 August 2023. The bill has received the Presidential assent followed by official gazette notification and has become a law of the land on 11 August 2023.

The Digital Personal Data Protection Act, 2023 (hereinafter referred to as 'DPDPA') lays down procedures to process personal data in a lawful manner and thereby empowers and protects the rights of Data Principals. Factors such as accountability, transparency, data minimisation, fairness, accuracy, and lawful processing of personal data have been reflected in the DPDPA. It addresses Data Principals as 'she/her', which is unseen in any Indian law till date and sets the tone in a new light.

This document delves into the various aspects of the DPDPA and aims to provide our point of view on its implications, challenges, and potential benefits.

2. Highlights of the DPDPA

The scope of the legislation only covers digitised personal data and excludes personal data that is made publicly available by the Data Principal.

Situations which were labelled earlier as deemed consent have been categorically permitted as "certain legitimate uses".

Cross-border transfers are now valid until certain transfers are explicitly restricted by the government.

A valid contract is mandatory for onboarding a Data Processor along with ensuring that due obligations including data deletion are abided by the Data Processors.

The retention period shall expire if the services for which consent has been provided are not utilised by Data Principal in the prescribed time period.

For five years from the commencement of the DPDPA, the Central Government has the power to exempt a Data Fiduciary or a class of Data Fiduciaries from any provision for a specific time-period.

Personal data of children should not be used for tracking, behavioral monitoring or targeted advertising.

Significant Data Fiduciaries will be required to appoint a Data Protection Officer (DPO), conduct periodic data protection impact assessments and engage independent auditors for carrying out data audits.

Consent managers are required to be registered with the Data Protection Board (herein after referred as 'Board') and are liable to Data Principals for enforcement of Data Principal rights.

Privacy Notice is to be provided in English or any other language specified in the Eighth schedule of the Constitution. However, this is limited to where processing is based on consent.

The DPDPA has introduced a unique Data Principal right – the right to nominate. Using this right, Data Principals can assign a representative to exercise their right in case of incapacity or death.

The DPDPA has omitted any kind of criminal liability for non-compliance with the law. The law imposes a financial penalty upto INR 250 crores per instance on Data Fiduciary. Further, penalty could also be imposed on Data Principals for breaches in observance of their duties defined under the law.

A phased implementation approach is proposed where the Government shall notify the sequential periodic implementation of different parts of the law or for different classes of Data Fiduciary.

3. Key stakeholders defined in the DPDPA

Data Principals

Individuals within the territory of India whose personal data is being processed.

Data Fiduciary

Data Fiduciaries are organisations deciding what data is to be collected, and how it is to be collected and the purposes for which it needs to be used.

Significant Data Fiduciary

Organisation that processes large volumes of sensitive data sets will be declared by the Government as Significant Data Fiduciary.

Data Processors

Data Processors are organisations that process data on behalf of Data Fiduciaries based on their instructions.

Consent Manager

Consent Managers would assist Data Principals and Data Fiduciaries to give, manage, review and withdraw consent.

4. Overview of the DPDPA

A. Applicability & Scope

1. **Territorial Scope:** The DPDPA applies to the processing of personal data collected in India which is in a digitised form or is collected in a non-digital format and has been thereafter, digitised.[1]
2. **Extraterritorial Scope:** The DPDPA also applies to the processing of digital personal data outside the territory of India, if the same is in connection with offering goods or services to Data Principals in India.[2] This would also fetch applicability for foreign entities operating websites in Indian national or regional languages aiming at targeting Indian Data Principals.
3. **Exempted Personal Data:** The DPDPA excludes personal data processed by individuals for any personal or domestic purpose, and personal data that is made publicly available by the Data Principal either by choice or under legal obligation.[3] This means that personal data made publicly available on social media and other prominent platforms by the Data Principals are excluded from the ambit of the DPDPA. However, this would not take away social media platforms' obligations in handling personal data generated through other means, including behavioral monitoring or direct messaging.

B. Sensitive personal data

The DPDPA is silent on further categorisation of personal data and sensitive personal data. This might be seen as a welcome move as organisations will be required to protect sensitive and non-sensitive personal data equally. However, this can also be concerning since sensitive personal data attributes such as biometric details are used for authentications and may require an enhanced layer of protection.

C. Exemptions

Certain processing activities have been exempted from obligations including, cross-border data transfer, all Data Fiduciary obligations, and Data Principals' rights-related obligations. These exempted processing activities include:[4]

1. Section 3(a), DPDPA
2. Section 3(b), DPDPA
3. Section 3(c), DPDPA
4. Section 17, DPDPA

D. Grounds of Processing

1. Consent

A valid consent under the DPDPA must be freely given, specific, informed, unconditional, and unambiguous, and must be established by an affirmative action by the Data Principal.[5] The addition of the term "unconditional" to the definition of consent could infer that the legislators aim at limiting consent to the primary purpose for which it is being collected. If this reasoning is adopted, it would suggest that where consent is combined for a secondary purpose it would be deemed conditional. For processing a minor's personal data, consent from their lawful guardian would be required.[6] However, consent is not absolute under the DPDPA, and the Data Principals have been empowered with the right to withdraw consent at any time during processing.[7]

2. Legitimate Use

Different basis of processing personal data such as legal obligation, medical emergencies, employment etc. are bundled into legitimate uses. Where personal data is processed under legitimate uses, other than where given voluntarily, the Data Principals will not have the right to erase, correct and access their personal data or withdraw their consent. The DPDPA takes a more narrow approach to the grounds for processing personal data in comparison to the prominent global privacy laws such as the General Data Protection Regulation (hereinafter referred as 'GDPR'), and does not explicitly prescribe contractual obligation. Considering that contracts are majorly used grounds for processing, businesses might be required to shift to consent which may be operationally challenging.

E. Privacy Notice

As per the DPDPA, the requirement of serving a notice applies only where the ground of processing is consent. Data Fiduciaries need to provide the details of personal data, the purpose for which it is processed, and the manner in which the Data Principal can exercise their rights under the DPDPA. The notice can be made available in English or any of the twenty-two languages specified in the Eighth Schedule of the Constitution.[9] Furthermore, the Data Principal needs to be informed on how they can file a complaint before the Board as a part of the notice. For processing activities where consent has been obtained before the commencement of law, a fresh privacy notice needs to be provided with the above requirements.

5. Section 6(1), DPDPA
6. Section 9(1), DPDPA
7. Section 6(4), DPDPA
8. Section 7, DPDPA
9. Twenty-two language specified in the Eighth Schedule of the Constitution include (1) Assamese, (2) Bengali, (3) Gujarati, (4 (1) Assamese, (2) Bengali, (3) Gujarati, (4) Hindi, (5) Kannada, (6) Kashmiri, (7) Konkani, (8) Malayalam, (9) Manipuri, (10) Marathi, (11) Nepali, (12) Oriya, (13) Punjabi, (14) Sanskrit, (15) Sindhi, (16) Tamil, (17) Telugu, (18) Urdu (19) Bodo, (20) Santhali, (21) Maithili and (22) Dogri.

F. Obligations of Data Fiduciary

The DPDPA imposes the following obligations on Data Fiduciaries:

01
Implement technical and organisational measures to safeguard personal data[10]

02
Determine legal ground of processing and obtain consent from Data Principals where required[11]

03
Provide a privacy notice while obtaining consent from Data Principals

04
Implement a mechanism for Data Principals to exercise their rights[13]

05
Implement a grievance redressal mechanism for handling queries from Data Principals[14]

06
Irrecoverably delete personal data after the purpose for which it was collected has expired or when the consent has been withdrawn[15]

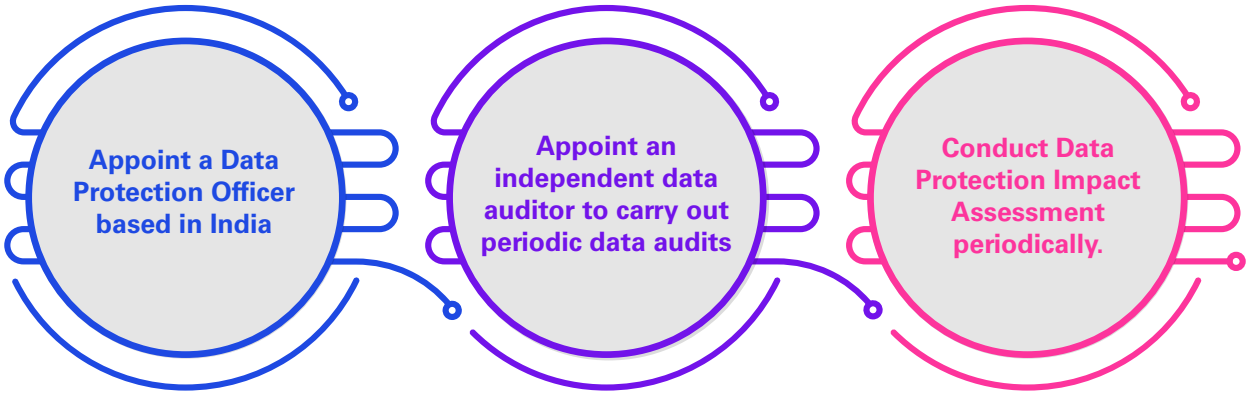
07
Have a breach management policy to notify the Data Protection Board and the Data Principals in accordance with proscribed timelines

08
Sign a valid contract with Data Processors to ensure key obligations are abided by them, including timely deletion of data

10. Section 8(4), DPDPA
11. Section 4(1), DPDPA
12. Section 5, DPDPA
13. Section 11, 12, 13, and 14, DPDPA
14. Section 8(10), DPDPA
15. Section 8(7), DPDPA
16. Section 8(6), DPDPA
17. Section 8(2), DPDPA

G. Obligations of Significant Data Fiduciary

In addition to the general obligations of a Data Fiduciary, a Significant Data Fiduciary must also: [18]



H. Retention & Deletion

The Data Fiduciaries are obligated to delete personal data once the purpose for which it was collected is fulfilled or when the Data Principal withdraws his/her consent, whichever is earlier.[19] Further, if the Data Principal does not approach the Data Fiduciary for a certain period as prescribed, the retention period shall be deemed to have expired, and the Data Fiduciary would be required to erase such personal data.[20] However, sectoral laws need to be considered when determining these aspects. For instance, record retention requirements from banking and telecom regulators which mandate different retention timelines.

I. Breach Notification

The DPDPA does not specify any particular time period within which the Data Fiduciary is required to inform the Data Protection Board and the Data Principals regarding data breaches. It is expected that the awaited DPDP Rules will prescribe breach notification timelines and it is anticipated that this will not be in conflict with the existing security incident notification timeline of 6 hours prescribed by the Computer Emergency Response Team (CERT).

J. Rights of Data Principal

Right to Withdraw Consent: Data Principals have been empowered with the right to cease processing by withdrawing their consent.[22] This would be facilitated by the Consent Manager who will play a significant role. However, a common technology architecture needs to be established between the Consent Mangers and Data Fiduciaries to make the process efficient.

Right to Grievance Redressal: Data Principals now have the right to grievance redressal.[23] The time period for responding to grievances shall be notified. Data Fiduciaries and Consent Managers will now be required to have a qualified person for addressing these grievances. The Board will only entertain matters which Data Fiduciaries or Consent Manager are unable to resolve.[24]

Right to Access Information: Data Principal has the right to obtain information on processing, the categories of personal data shared and identities of all the Data Processors with whom the personal data has been shared.[25]

Right to Nominate: This is a unique right that has not been seen in any other prominent privacy regulations, including the GDPR. A representative in case of incapacity or death of the Data Principal can be assigned to exercise their right.[26] From an ethical and moral standpoint, this is a milestone in recognising the human rights of an individual's identifiable property after death rather than it being in the public domain and used by anyone and everyone.

19. Section 8(7), DPDPA
20. Section 8(8), DPDPA
21. Section 8(6), DPDPA
22. Section 6(7), DPDPA
23. Section 8(10), and Section 13, DPDPA
24. Section 13(3), DDPDPA
25. Section 11, DPDPA
26. Section 14, DPDPA

Right to Correction and Erasure of Personal Data: The Data Principal can request Data Fiduciaries to correct, complete, update, and delete their personal data.[27]

Exceptions: Right to access, and right to correction and erasure of personal data is applicable only where the ground of processing is consent. It is pertinent to note that in all the versions of India's privacy regulation, the DPDPA is the first version which provides rights based on the grounds of processing personal data.

K. Cross-border data transfer

The DPDPA has eased the cross-border data transfer requirement where the Data Fiduciaries can transfer personal data to other countries unless notified and restricted by the Central Government.[28] This could be a relief for the Data Fiduciaries as the need to enforce restrictions and related controls would be limited to the countries notified and thus will have limited impact on the ongoing business. Shifting to the blacklisting mechanism is seen as a relieving move but there needs to be some guidelines on criteria being considered.

L. Processing Children's Personal Data

Consent from lawful guardian would be required for processing personal data of children and people with disability.[29] Organisations are prohibited from processing personal data for tracking, behavioral monitoring or targeted advertising.[30] The law also provides the government with the power to provide a lower age limit for applicability if the Data Fiduciary processes the personal data of children in a verifiably safe manner.[31] Although this is a flexible regime, stronger rules in terms of criteria for evaluating the Data Fiduciary need to be implemented to ensure that it doesn't lead to more breaches of data pertaining to children.

M. Data Protection Board

The DPDPA lays down the functions of the Board and provides aspects such as the qualifications of the chairperson and disqualifications of board members. A key point is that the law addresses the resignation process and filling of vacancies which can lead to efficient functioning.[32] The DPDPA has also clarified that funds realised from penalties will be credited to the Consolidated Fund of India.[33] Additionally, the Central Government will now have the power to block a Data Fiduciary's platform.[34] The Board will also have the power to hear complaints against Consent Managers. Like the GDPR, the Central Government can also prescribe threshold criteria for compensating a Data Principal due to any detrimental impact from a data breach.

N. Implication to Right to Information

The DPDPA is also amending relevant aspects of The Right to Information, Act, 2005 (hereinafter referred to as 'RTI Act').[35] Information containing personal data which could be denied under certain circumstances will now be denied under all circumstances, subject to the other provision of the DPDPA. While the RTI Act was passed with the aim of transparency, the DPDPA is now aiming to strike a balance by exempting all personal data of Data Principals such as employees in public authorities. This can also simply mean that such personal data will be masked and still allow non-personal data can be shared under the RTI Act.

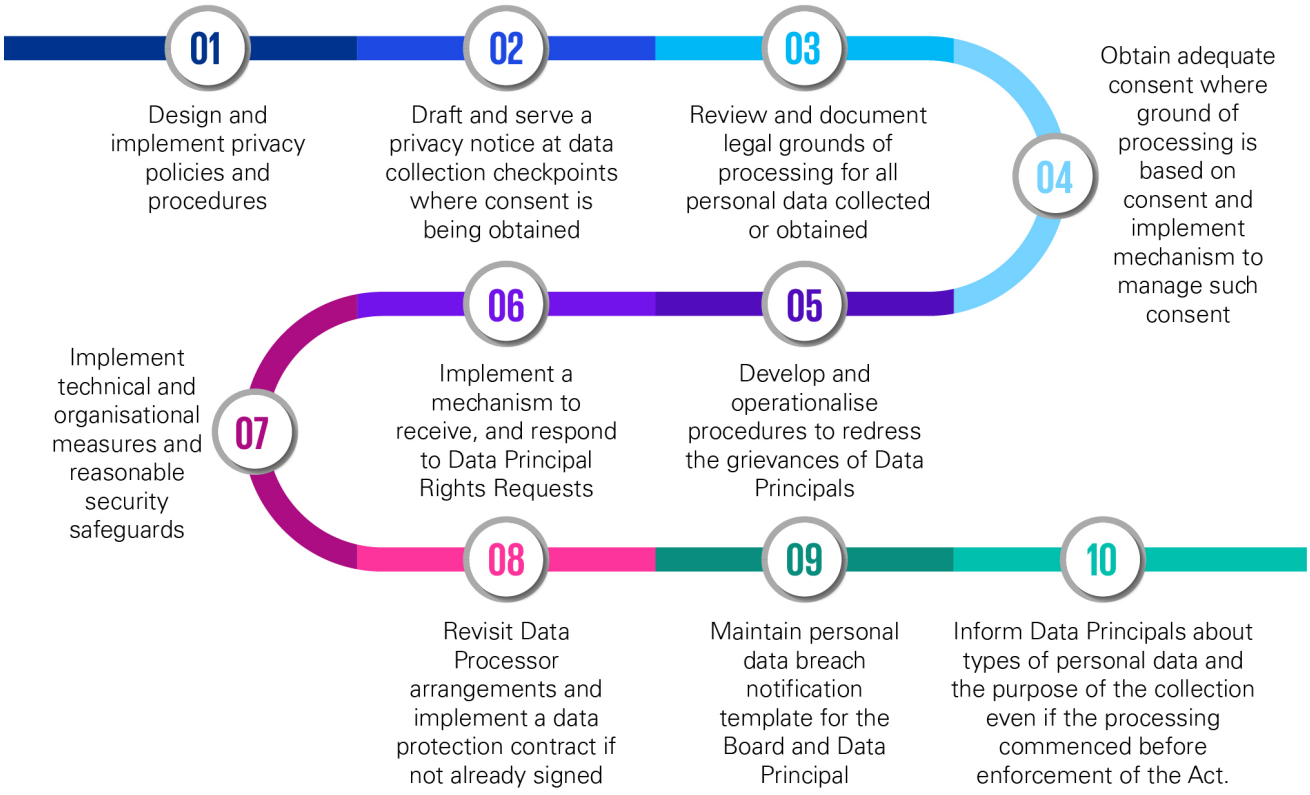
O. Penalties

In comparison to the 2022 DPDP Bill, the DPDPA has reduced the upper limit of a penalty from INR 500 crores to INR 250 crores. The DPDPA imposes penalty for non-compliance on Data Principals, Data Fiduciaries, Significant Data Fiduciaries and Consent Managers. The legislation has adopted a layered penalty mechanism, where severe violations leading to data breaches, have been levied with the highest penalty of ₹ 250 crores.[36] Data Principals will also be imposed with a fine of ₹ 10,000 if they violate their duties defined under the Act.[37]

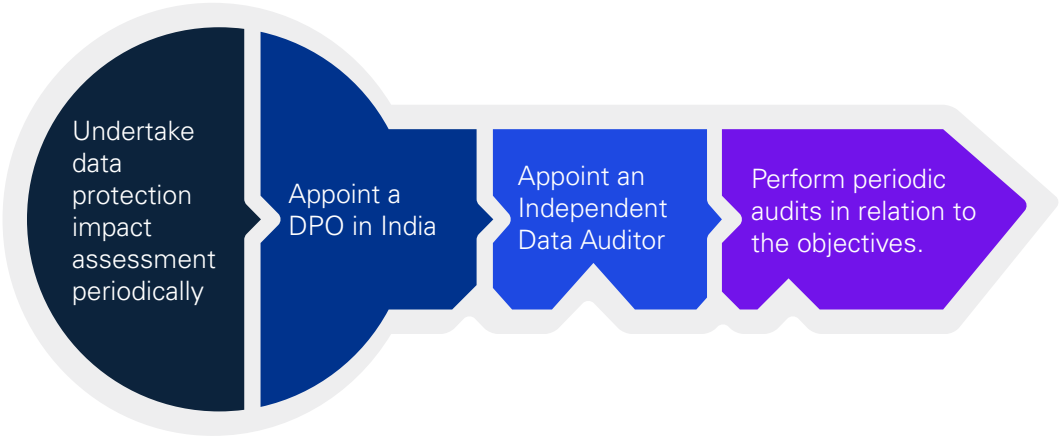
---

27. Section 12, DPDPA
28. Section 16, DPDPA
29. Section 9(1), DPDPA
30. Section 9(3), DPDPA
31. Section 9(5), DPDPA
32. Section 22, DPDPA
33. Section 34, DPDPA
34. Section 37, DPDPA
35. Section 44(3), DPDPA
36. Section 33 and The Schedule, DPDPA
37. Section 33 and The Schedule, DPDPA

5. A typical DPDPA privacy compliance journey



If a Significant Data Fiduciary, the following steps will need to be adhered to additionally:



19. Section 8(7), DPDPA
20. Section 8(8), DPDPA
21. Section 8(6), DPDPA
22. Section 6(7), DPDPA
23. Section 8(10), and Section 13, DPDPA
24. Section 13(3), DDPDPA
25. Section 11, DPDPA

6. Positive aspects of the DPDPA

Boosts growth and innovation: The DPDPA has a significant effect on the business sector and was inevitable considering the speed of digitisation in India and volumes of personal data being processed. Implementation of the DPDPA will boost consumer trust, cross-border trade, lawful processing and will thus enhance India's economy and digital innovation.

Empowers Data Principals: Individuals now have the right over their personal data to withdraw their consent, seek grievance redressal, correct, access, and update their personal data and appoint a nominee for the same. This empowers Data Principals to have more control over their personal data along with ensuring transparency.

Provides alternative to consent based processing: The legitimate uses involve different purposes for processing such as complying with laws, and court orders, responding to medical emergencies, ensuring safety, and defending rights. These permitted purposes can enable businesses to reduce their burden by relying on grounds of processing, other than consent. It will save costs in implementing additional mechanisms for consent management.

Distributed liability for organisation: The DPDPA allows both, Data Fiduciary and Consent Managers to be held liable before the Board when they fail in their carrying out their respective responsibilities. This eases consent-related compliance and liability for Data Fiduciaries.

Effective Data Processor governance: The DPDPA requires Data Fiduciaries to engage Data Processors only under an agreement. The Data Processor can now be held accountable under contract for failing to assist a Data Fiduciary in obligations. This can help Data Fiduciaries plan for their risk appetite and set off risk with obligations which are shared responsibilities with the Data Processor.

Increased accountability: Significant Data Fiduciaries have an additional obligation to conduct Data Protection Impact Assessments. This addition is required as it applies to Data Fiduciaries which process personal data in a manner that can lead to a higher risk to the Data Principal. The requirement to assess the risk to the rights of individuals as a part of the Data Protection Impact Assessment will bring a balance between the risks of processing personal data and business interests.

Ease in implementation: A phased implementation proposed in the DPDPA gives organisations the time to plan their changes for complying with provisions of the DPDPA and reduces resources required for compliance with the DPDPA.

Relaxed cross-border transfer: The DPDPA has provided a minimally restrictive approach to cross-border data transfers. This can help businesses minimise costs on transfer mechanisms and consequently contribute to business profits.

7. Potential challenges in implementation

Data Processing under contractual obligations: Moving away from deemed consent, the law now seeks to require Data Fiduciaries to process personal data on consent and certain legitimate uses. It is seen that contractual obligation has not been directly categorised under legitimate uses. The DPDP Rules or the Board should shed light on whether businesses can enforce contracts under legitimate uses or if they would be required to resort to consent for processing personal data

Limitation on Data Principal rights: The rights of Data Principals with respect to access, correction, and erasure do not apply when data is processed for legitimate uses except when the Data Principal voluntarily provides their personal data. While the rights are now made available, it discriminates against individuals whose personal data has been collected for legitimate uses and not with their consent.

No obligation for data mapping and data inventorisation: The law does not mandate maintaining records of processing activities or data maps to identify how the personal data is flowing within the organisation infrastructure and where it is being stored. In the absence of such mandates, managing Data Principal rights or auditing larger businesses can be a challenge.

Exemption on classes of Data Fiduciary: The Central Government can exempt a Data Fiduciary or a class of Data Fiduciaries from certain obligations under the DPDPA. However, the rationale behind such exemptions is unclear.

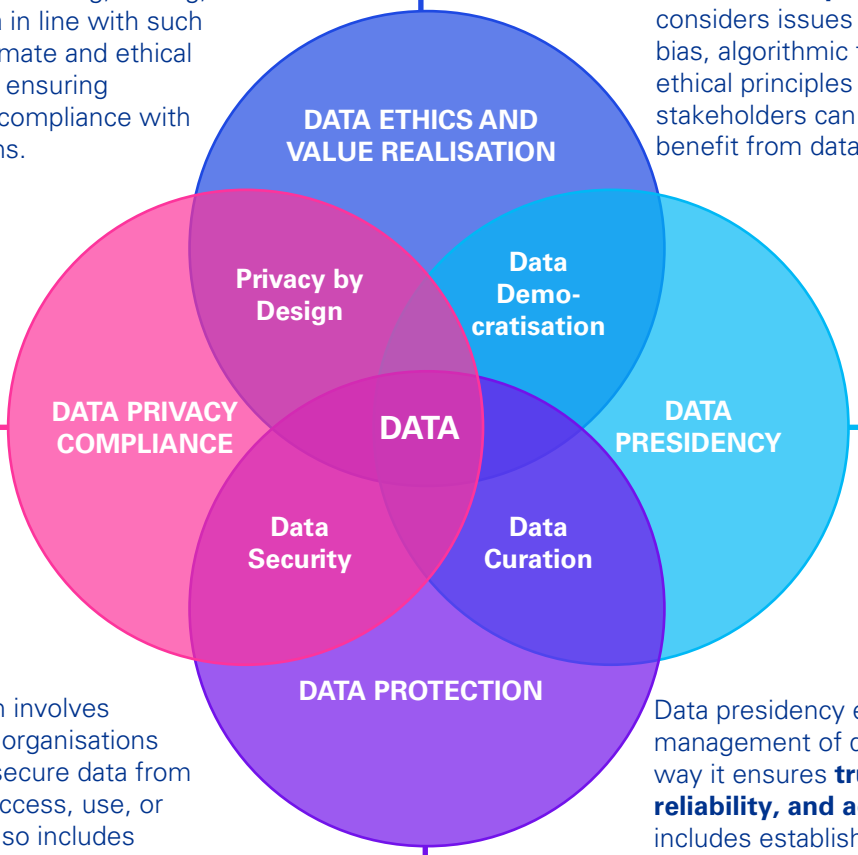
Processing of children's personal data: If the central government is satisfied that a Data Fiduciary processes children's personal data in a manner that is "verifiably safe", the Central Government can exempt such Data Fiduciary from any or all obligations of processing children's data above a certain age. However, what would constitute as verifiably safe is unclear and thus can be detrimental to the rights protection of children.

8. How to turn obligation into opportunity?

Organisations should not only view DPDPA 2023 to be a compliance mandate but consider this an opportunity to enable business. Adopting the data trust framework helps organisations to have better control of their data thereby maintaining the balance between value protection and value creation while staying on the right side of compliance and gaining competitive advantage.

Data privacy compliance entails complying with relevant laws, regulations, and guidelines for **data protection and privacy.** This involves collecting, storing, and using data in line with such laws, for legitimate and ethical purposes, and ensuring stakeholders' compliance with data regulations.

Data ethics and value realisation involves principles and values guiding ethical data use, including **transparency, fairness, and privacy.** It considers issues such as system bias, algorithmic fairness, and ethical principles that ensure stakeholders can generate and benefit from data value.



Data protection involves measures that organisations implement to secure data from unauthorised access, use, or disclosure. It also includes protocols for responding to security incidents and breaches and notifying the stakeholders as required by law.

Data presidency encompasses management of data assets in a way it ensures **trust, reliability, and accuracy.** It includes establishing processes for data collection, storage, sharing, and analysis, and implementing supporting tools and technologies.

9. Frequently Asked Questions

Who should be concerned with the DPDPA?

Any company or organisation processing digital personal data of Indian Data Principals. Processing entails the collection, organisation, structuring, storage, sharing, disclosure by transmission, erasure, destruction, or any other automated operation performed on personal data.

What happens to data collected prior to commencement of the DPDPA?

Upon commencement of the DPDPA, organisations need to issue a fresh notice to Data Principals and provide them with the details of personal data, the purpose for which they are processed, the rights of Data Principals, and how they can file a complaint with the Board.

For organisations that are GDPR compliant, what additional measures need to be taken for the DPDPA compliance?

GDPR compliant organisations will need to additionally:

- Review and determine the legal ground of processing for all personal data collected
- Update Data Principal rights mechanism by accommodating the right to nominate
- Implement a grievance redressal mechanism
- Review and adjust data deletions schedules as per provisions of the DPDPA
- Revisit the onboarded Data Processor arrangements and review the data protection clauses if not already signed
- Appoint a Data Protection Officer in India, if the organisation is a Significant Data Fiduciary
- Ensure that privacy notices provided to Data Principals are made available in English or in any of the twenty-two languages specified under the Eighth Schedule of the Indian Constitution
- Conduct data protection impact assessment periodically and appoint an independent auditor, if the organisation is a Significant Data Fiduciary.

Is cross-border data transfer permitted?

Yes, an organisation can share/transfer data outside of India. However, certain transfers can be restricted by the Board. Further, organisations need to take into account the sectoral regulations imposing restrictions on such transfers.

Are startups in India exempted from the DPDPA?

Startups are not exempted from the DPDPA. However, the certain class of Data Fiduciaries such as startups can be exempted of certain obligations of the DPDPA, based on the volume and nature of personal data processed.

Are there any implementation timelines prescribed?

The DPDPA proposes a phased implementation. The Board shall be notifying the sequential periodic implementation of the clauses.

Do organisations need to register with the Data Protection Board?

Data Fiduciaries or Data Processors are not required to be registered with the Board. However, Consent Managers have this requirement. The procedure for registering with the Board is yet to be prescribed.

How are penalties enforced by the Data Protection Board?

The Board acts as an independent body and can act on a compliant made by a Data Principal for non-compliance. Based on the complaint, the Board can assess the complaint, launch and inquiry and pass an order against a Data Fiduciary or a Consent Manager, if they are non-compliant An appeal on the decision by the Board can be made to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

What is the time period for notifying personal data breaches to the Data Protection Board and Data Principal?

The manner and time period within which a personal data breach is to be notified is yet to be prescribed.

Does the Data Protection Officer need to be based out of India?

If the organisation is notified by the government as a Significant Data Fiduciary, a Data Protection Officer needs who is based out of India needs to be appointed.

Acknowledgments:

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

Amrita Kumar

Karthik JCS

Samya Gupta

Divya Kakarya

Praveen Raghuvanshi

Shubhankar Mathur

Design, compliance and support

Prajakta Talpade

Karthika Prabasankar

Nisha Fernandes

KPMG in India contacts:

Atul Gupta
Partner & Head - Digital Trust
T: +91 98100 81050
E: atulgupta@kpmg.com

Mayuran Palanisamy
Partner - Digital Trust
National Privacy Lead
T: +91 96000 57046
E: mpalanisamy@kpmg.com

Nitin Shah
Partner - Digital Trust
Cyber Strategy & Governance
T: +91 95602 44888
E: nitinshah@kpmg.com

Jignesh Oza
Partner - Digital Trust
Data Privacy
T: +91 99675 45665
E: joza@kpmg.com

Rupak Nagarajan
Director - Digital Trust
Data Privacy
T: +91 98411 24470
E: rupak@kpmg.com

kpmg.com/in

kpmg.com/in/socialmedia

30 years and beyond