The Digital Personal Data Protection Act 2023
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

- **2017-2018**
  - Draft Data Protection Bill

- **2019**
  - Introduction of the Personal Data Protection Bill (PDPB)

- **2020**
  - Parliamentary Committee report on PDPB

- **2021**
  - Withdrawal of PDPB, 2019 and release of draft Digital Personal Data Protection Bill

- **2022**
  - July - Cabinet approval of the DPDP Bill
  - August - DBDP Bill, 2023 was passed by both houses of the Parliament and received Presidential assent and notified in gazette to become an enforceable Act

- **2023**

© 2023 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The Digital Personal Data Protection Act – Overview (1/3)

Key obligations

**Data Principal Rights Mechanism**
Implement a mechanism for Data Principals to exercise their rights

**Security**
Implement technical and organisational measures to safeguard personal data

**Onboarding Data Processors**
Sign a valid contract and ensure key obligations are abided by including deleting data as required

**Retention and Deletion**
Irrecoverably delete personal data after the purpose for which it was collected has expired

**Data Breach**
Notify personal data breaches to Data Protection Board and affected individuals

**Greivance Redressal**
Implement a grievance redressal mechanism for handling queries from Data Principals

**Key stakeholders defined in the Act**

- **Data Principal**
  The Individual to whom personal data relates

- **Data Fiduciary**
  Defines the purposes and means of personal data processing

- **Data Processor**
  Processes personal data on behalf of the Data Fiduciary

- **Data Protection Officer**
  Individual appointed by Significant Data Fiduciary

- **Consent Manager**
  Organisation managing the consent of Data Principals

© 2023 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The Digital Personal Data Protection Act – Overview (2/3)

**Rights of Data Principals**

**Right To Grievance Redressal**
The Data Fiduciary 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 the Data Fiduciaries and the 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.

---

**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:
  - Digitized form
  - Non-digital form and digitized subsequently.

Financial penalties up to INR 250 crore per instance.

Data Principal could also be fined up to INR 10 thousand in case of violations of their duties.
There are two grounds of processing defined 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. In case of children, consent shall be obtained from the parent or the lawful guardian.

**Consent should be**

- Freely Given
- Specific
- Unconditional & Unambiguous

**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.

**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

**FAQ**

- Who will provide consent? Data Principal
- Who will ask for consent? Data Fiduciary
- How consent should be requested?
  - In clear and plain language
  - Using itemised notice
- How can consent be withdrawn?
  - By contacting Data Fiduciary or Consent Manager

© 2023 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
Key changes introduced in the DPDPA 2023 (1/2)

The DPDPA 2023 was passed by the Lower House of Parliament (the Lok Sabha) and the Upper House of Parliament (the Rajya Sabha) in August 2023. Here are key amends made in the current version of the Act:

Privacy Notice
Enhancement in the content of the privacy notice must include how the individuals can exercise their rights and how a complaint to the Data Protection Board can be made.

Onboarding Data Processors
A valid contract is mandatory for onboarding Data Processor.

Grounds of Processing
Situations under which implicit consent was deemed previously have been categorically permitted as "legitimate uses".

Data Retention
Obligation on data fiduciary to ensure data is deleted by an onboarded processor. The retention period shall expire if the services for which consent has been provided are not utilized by Data Principal in the prescribed time period.
Key changes introduced in the DPDPA 2023 (2/2)

Data Protection Impact Assessment (DPIA)
DPIA has been made periodically mandatory for significant data fiduciaries. Further, steps on what should be made a part of the DPIA have been elaborated to include a description and purpose of processing, management of risks to individuals, etc.

Grievance Redressal
Grievance redressal mechanism to be set up and provided by both Data Fiduciary and Consent Manager. The timeline within which the grievance to be addressed to be specified by the Data Protection Board. Data Principal can reach out to Board with their grievances subject to exhausting all remedies.

Cross-Border Data Transfer
Whitelisting approach for transferring data outside India is replaced by a blacklisting approach. Cross-border transfer is valid until certain transfers are explicitly restricted by the government.
What’s next? - The road to compliance

- Appoint a [DPO](#) and publish business contact information*
- Design and implement privacy policies and procedures
- Draft a privacy notice to inform the Data Principals
- Implement technical and organisational measures and reasonable security safeguards
- Inform Data Principals about types of personal data and the purpose of the collection
- Enforcing procedures to handle Data Principal Rights requests / grievances and data breaches
- Undertake Data Protection Impact Assessment *
- Involve a Data Processor (if required) pursuant to a valid contract
- Perform periodic audits *

* Applicable to Significant Data Fiduciary only

---

© 2023 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
Please feel free to reach out to us in case of any queries, we look forward to hear from you.

Atul Gupta
Partner and Head, Digital Trust and Cyber Security
KPMG in India
Email: atulgupta@kpmg.com

Srinivas Potharaju
National Co-Head, Digital Risk Security and Governance (DRSG)
KPMG in India
Email: srinivasbp@kpmg.com

Mayuran Palanisamy
Partner, National Head, Data Privacy
KPMG in India
Email: mpalanisamy@kpmg.com

Nitin Shah
Partner, Cyber Security
KPMG in India
Email: nitinshah@kpmg.com

Kunal Pande
National Co-Head, Digital Risk Security and Governance (DRSG)
KPMG in India
Email: kpande@kpmg.com

Jignesh Oza
Partner, Cyber Security
KPMG in India
Email: joza@kpmg.com

Rupak Nagarajan
Director, Cyber Security
KPMG in India
Email: rupak@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

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.
© 2023 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.
This document is for e-communication only.