India Digital Personal Data Protection Act, 2023 (DPDP Act)

What is DPDP Act?

This Act governs the processing of digital personal data in India, regardless of whether the data was originally collected in digital or non-digital format and subsequently digitized.

Who is impacted by the DPDP Act?

Any company processing digital personal data related to offering of goods or services to people within India – regardless of where the company is based.

What is "personal data"?

Any data about an individual who is identifiable by or in relation to such data.

- DPDP Act effective from 13 November 2025 in three phases:

  First set upon official notification; second set after one year; and final set 18 months from the date of notification.

Tough penalties*

Up to INR250 crore for failure to have reasonable security safeguards

Up to INR200 crore for data breach notification failure

Up to INR200 crore for violation of children's data

- Data Principals have the right of access, correction, completion, updating and erasure. Additional rights of grievance redressal and nomination.

- Organizations to be categorized as

Data Fiduciary

Significant Data Fiduciary

Lawful processing include – Legitimate use and Consent

- freely given
- informed
- unambiguous
- affirmative action

Provisions for verifiable consent for processing children's personal data

Obligations of Data Fiduciary

Data Fiduciary is responsible for any processing undertaken by it or on its behalf by a Data Processor

- Notice
- Consent
- Storage period limitation
- Reasonable safeguards
- Breach notifications
- Contracts with Data Processors

Obligations of Significant Data Fiduciary

Specific obligations include –

- Appointing a Data Protection Officer (DPO) based in India
- Appointing an Independent Data Auditor
- Conducting Data Protection Impact Assessment (DPIA)
- Regular audits

* Cumulative penalties can be more than INR250 crore

EY

Shape the future with confidence

Digital Personal Data Protection Rules, 2025

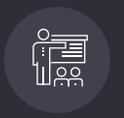
The Digital Personal Data Protection Rules, 2025 ('Rules') were notified on 13 November 2025. However, Rules 3, 5 to 16, 22 and 23 - relating to compliance and enforcement - shall come into force after 18 months, giving time to stakeholders for technical and operational readiness

Notice given by Data Fiduciary to Data Principal

- Independent in clear and plain language
- Include itemised description
- Give particular communication link to exercise their rights under the Act
- In English or any of the 22 languages specified in the Eighth Schedule of Indian Constitution

Data Principal's Rights

- Access, correction, completion, updating, erasure, grievance redressal (within 90 days) and nomination
- Can furnish business contact information of DPO or any other person responsible for ensuring rights of Data Principals



Personal data of children/ person with disability

- Verifiable consent and identity verification of parent/ lawful guardian as prescribed

Personal data breach

- 72 hours to furnish report to Data Protection Board (DPB)
- Intimation, without delay, to the concerned Data Principal and DPB

Data retention timeline

- 3 years, based on last date of approach, for E-commerce, gaming, social media intermediaries
- For others: 1 year or as required by any law

Reasonable security safeguards

- Encryption, obfuscation, masking, maintaining data backups or use of virtual tokens mapped to personal data
- Access control management and maintenance of access logs
- In case of unauthorized access, retention of personal data and logs for a period of 1 year or as required by any law

Significant Data Fiduciary (SDF)

- Conduct Data Protection Impact Assessment and report significant findings to DPB
- Annual audit and report to be furnished to DPB
- Observe due diligence of algorithmic software
- Certain personal and traffic data not to be transferred outside India
- Government of India can carry out an assessment to classify any Data Fiduciary as SDF

Exemptions

- Research, statistical and archiving purposes as specified
- Processing of children's data subject to conditions prescribed in Fourth Schedule: Clinical, mental health, educational establishments in respect of children/ person with disability

Transfer of personal data outside India

- Transfer of personal data outside India is allowed subject to restrictions to be specified by central government

Consent Manager

- First Schedule lays down requirements and obligations of registering as a Consent Manager with the DPB
- Registration and obligations commence from 13 November 2026

Source:https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf

Way Forward

Roadmap to be compliant with DPDP Act and Rules

Companies need to adopt below mentioned steps depending on where they are in their journey. With over a decade of experience on providing Data Privacy and Protection services on 40+ global regulations across all sectors in India; EY is well positioned to help you in your end to end data privacy and protection journey

01 Data Privacy Assessment

Assess the current Data Privacy posture, working practices and documentation against the requirement of DPDP Act and Rules

02 Data Discovery and Mapping

Identify the personal data touch points and conduct data discovery and mapping activities

03 RoPA and Data Flow Diagram

Document personal data processing activities and its flow across various processes, systems, applications, third parties, etc.

04 Consents and Notices

Prepare consents, cookie banners, cookie policies and privacy notices to be implemented across touchpoints where personal data is collected

05 Privacy Impact Assessment

Identify data privacy risks by performing privacy impact assessments for processing activities and define controls to be implemented for mitigation

11 Training and awareness

06 Third-Party Risk Management

For third parties processing personal data, ensure reasonable safeguards are implemented through inclusion in contracts

07 Technical Safeguards

Identify and implement the required technical safeguards to enable protection of personal data from data breaches

08 Data Protection Office Setup

Set up a data protection office by identifying the right team accountable and responsible for enabling compliance within the organization

09 Implementation and Automation

Implement the controls required to achieve compliance and identify opportunities for automation for efficient compliance management

10 Monitoring and Sustenance

Implement a periodic monitoring program to assess compliance at various intervals to sustain what has been implemented

Key actions: Organizations in the journey of Data Protection compliance can be -

Starting fresh

- Assess the applicability from India DPDPA perspective and initiate personal data discovery
- Follow the steps described in the roadmap from start to end
- Perform ongoing monitoring and sustenance once implementation is complete

Globally aligned with international regulations

- Update / create unified privacy compliance framework basis DPDP
- Perform gap assessment and data discovery to identify gaps and data processing activities
- Update data protection and privacy policies and procedures
- Implement controls and perform ongoing monitoring

Started DPDPA compliance but not there yet

- Perform incremental gap assessment to identify the changes and updates
- Update existing documents, if already created, basis additional obligations as per the DPDP Rules
- Implement and roll out data protection controls
- Perform ongoing monitoring and sustenance