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

What is the DPDP Act?

The Digital Personal Data Protection (DPDP) Act, 2023 governs the processing of digital personal data in India. It applies regardless of whether the data was originally collected in digital or non-digital form and later digitized.

When does the Act come into effect?

The DPDP Act comes into force from 13 November 2025 and will be implemented in three phases:

- First set upon official notification
- Second set after one year
- Final set within 18 months from the date of notification

Who is impacted?

Any organization processing digital personal data related to offering goods or services to individuals in India is covered under the Act irrespective of where the organization is located.

Penalties for Non-Compliance

The Act prescribes strict financial penalties, including:

- Up to ₹250 crore for failure to implement reasonable security safeguards
- Up to ₹200 crore for failure to notify data breaches
- Up to ₹200 crore for violations involving children's personal data

Rights of Data Principals

Individuals (Data Principals) have the right to:

- Access their personal data
- Correct and update data
- Complete incomplete data
- Erase personal data
- Seek grievance redressal
- Nominate a representative

Obligations of Significant Data Fiduciaries

Organizations classified as Significant Data Fiduciaries must additionally:

- Appoint a Data Protection Officer (DPO) based in India
- Appoint an Independent Data Auditor
- Conduct Data Protection Impact Assessments (DPIA)
- Undergo regular audits

Source - Government of India

Digital Personal Data Protection Rules, 2025

Progressive

The Digital Personal Data Protection Rules, 2025 (“Rules”) were notified on 13 November 2025. However, Rules 3, 5–16, 22, and 23 - which pertain to compliance and enforcement—will take effect after an 18-month period, allowing stakeholders sufficient time to achieve technical and operational readiness.

Notice to Data Principals

- Standalone notice in clear, plain language
- Itemised details of data collected and purpose
- Dedicated link to exercise rights
- Available in English or Eighth Schedule languages

Rights of Data Principals

- Access, correction, updating, and erasure of data
- Grievance redressal within prescribed timelines
- Contact details of DPO or responsible officer required

Children & Persons with Disability Data

- Verifiable consent of parent or lawful guardian mandatory
- Additional safeguards as prescribed under the Rules
- Age and identity verification mechanisms to prevent misuse

Personal Data Breach

- Report personal data breaches to the Data Protection Board (DPB) without delay
- Notify affected Data Principals as soon as possible
- Disclose the nature, scope, and potential impact of the breach

Data Retention & Deletion

- Retain data only as long as required for its stated purpose
- Delete data once the purpose is met or consent is withdrawn, unless legally required
- Retention periods may vary by category, as notified

Security Safeguards

- Implement reasonable security safeguards including encryption, access controls, logging, monitoring, and secure backups
- Safeguards should be commensurate with the volume and sensitivity of personal data processed

Unauthorized Access Handling

- Maintain logs and records relating to access, processing, and security incidents
- Retain logs and related information for the period specified under the Rules
- Support investigations, audits, and compliance assessments

Significant Data Fiduciary (SDF)

- Designated by the Government based on data volume, sensitivity, and risk
- Required to conduct DPIA and appoint a Data Protection Officer
- Subject to enhanced compliance, audits, and reporting obligations

Cross-Border Data Transfer

- Permitted subject to conditions and restrictions notified by the Government
- Requires ongoing monitoring of approved countries and transfer requirements

Consent Manager

- Registered entity enabling Data Principals to give, manage, and withdraw consent
- Operates under regulatory oversight of the Data Protection Board

Source - Government of India

Timelines and obligations are subject to category-specific notifications under the Digital Personal Data Protection Rules, 2025.

Roadmap to be compliant with DPDP Act and Rules

Progressive

Companies should adopt the steps outlined below based on their current stage of maturity. With over 28 years of experience and 24/7 operational support, Progressive TechServe is well positioned to support organizations throughout their end-to-end data privacy and protection journey across multiple sectors and global regulations.

01 Data Privacy Assessment
Assess the current data privacy posture, existing policies, processes, and documentation against DPDP Act and Rules requirements.

02 Data Discovery & Mapping
Identify where personal data resides across systems, applications, databases, vendors, and business functions.

03 RoPA & Data Flow Mapping
Document Records of Processing Activities (RoPA) and map data flows across collection points, internal systems, and third parties.

04 Notices & Consent Framework
Draft and implement privacy notices, consent mechanisms, cookie banners, and communication channels across all data collection touchpoints.

05 Privacy Impact Assessment (PIA / DPIA)
Identify privacy risks for data processing activities and define controls to mitigate operational, legal, and security risks.

06 Third-Party Risk Management
Assess vendors and processors handling personal data and update contracts to include DPDP-compliant safeguards and obligations.

07 Technical & Security Safeguards
Implement encryption, access controls, logging, monitoring, masking, backups, and breach response mechanisms.

08 Data Protection Office Setup
Appoint a Data Protection Officer (DPO) or responsible officer and define governance, accountability, and escalation processes.

09 Implementation & Automation
Operationalize controls, enable consent and rights management workflows, and automate compliance where possible.

10 Monitoring, Audit & Sustenance
Conduct periodic audits, monitor compliance continuously, address gaps, and update controls as regulations evolve.