Navigating India's Digital Personal Data Protection Rules, 2025: Strategic POV

November 2025

ALVAREZ & MARSAL

LEADERSHIP. ACTION. RESULTS.℠

Background

Enacted in 2023, India's Digital Personal Data Protection Act (DPDPA) is a landmark in the country's digital regulation landscape. It establishes a citizen-centric framework for responsible personal data stewardship. The newly notified DPDP Rules, 2025[1], provide actionable clarity for both public- and private-sector entities, focusing on practical compliance, ethical processing, and risk minimization. Together, these rules elevate privacy from a conceptual right to an operational standard, embedding oversight and transparency into every data-driven process.

Applicability of DPDPA

The DPDPA, 2023, applies to all public- and private-sector entities that process digital personal data within India's territory, including personal data originally collected offline but subsequently digitized. It also extends to foreign organizations offering goods or services to individuals located in India.

Essential Roles Outlined in the DPDPA

- **Data Principal:** Any person whose data is being processed is empowered with rights to information, correction, and erasure.
- **Data Fiduciary:** The entity that determines the purpose and methods for processing personal data and bears primary accountability for compliance.
- **Consent Manager:** A registered platform enabling individuals' granular control over permissions and withdrawals.
- **Significant Data Fiduciary (SDF):** Entities with large digital footprints or handling sensitive information; subject to advanced risk, audits, and impact obligations.
- **Data Protection Officer (DPO):** The designated individual responsible for implementing data protection strategy and ensuring organizational compliance with the DPDPA and its rules.
- **Data Protection Board of India (DPB):** The statutory body established under Section 18 to enforce the Act and adjudicate breaches.

Phased Enforcement Timeline

Phase and Date	Rules Activated
Phase 1 – Immediate (Nov 14, 2025)	Rule 1, 2, 17-21
Phase 2 – After 12 Months (Nov 2026)	Rule 4
Phase 3 – After 18 Months (May 2027)	Rule 3, 5-16, 22-23

Key Obligations Under the DPDP Rules, 2025

Rule 3 – Privacy Notices	▪ **Independent and Clear:** Notices must be standalone and drafted in plain language.
	▪ **Key Details:** Itemized personal data + purpose of processing.
	▪ **Access Info:** Provide an accessible link to website/app with clear steps to:
	  ▪ Withdraw consent;
	  ▪ Exercise rights under the Act; and
	  ▪ File complaints or grievances.

Rule 4 – Consent Managers	▪ **Eligibility and Application:** Entities meeting criteria in First Schedule Part A may apply to the Board, with required documentation.
	▪ **Board's Role:** The Board verifies compliance, then either registers and publishes Consent Manager details or rejects the application with reasons.
	▪ **Consent Manager Duties (First Schedule Part B):**
	  ▪ Enable users to give, review, and withdraw consent through a website or app.
	  ▪ Ensure shared data remains unreadable to the Consent Manager and implement safeguards against breaches.
	  ▪ Retain consent and data-sharing records for seven years in machine-readable format.
	  ▪ Avoid subcontracting of obligations that create conflicts of interest.
	▪ **Compliance Monitoring:** The Board may direct corrective actions for non-adherence after hearing the Consent Manager.
	▪ **Enforcement Actions:** The Board may suspend/cancel registration and issue directions to protect Data Principals.
	▪ **Information Requests:** Consent Manager must promptly provide any information requested by the Board.

Rule 5 – Processing of Personal Data by the State and Its Instrumentalities	▪ **Processing Standards:** State actors must comply with the Second Schedule's minimum technical and organizational measures for personal data processing.
	▪ It mandates that personal data must be processed lawfully and transparently, limited to necessary data for specified purposes, maintained accurately, securely protected, retained only as long as needed, with timely breach notification, clear communication to data principals, and accountability of the entity controlling the data processing.
	▪ **Scope of Provision:** Applies to processing undertaken while administering subsidies, benefits, services, certificates, licences, or permits:
	  ▪ **Under Law:** Processing by State or its instrumentalities exercising legal powers.
	  ▪ **Under Policy:** Processing conducted in accordance with Central/State Government policies or instructions.
	  ▪ **Using Public Funds:** Expenditure from Consolidated Fund of India/State or public accounts, or funds of local authorities.

Rule 6 – Reasonable Security Safeguards	▪ **Data Fiduciary Responsibility:** Data Fiduciaries must protect personal data in its possession, or processed on their behalf by a Data Processor, as per the Minimum-Security Safeguards (detailed in subsequent section).

Rule 7 – Breach Notification	▪ **Notify Affected Data Principals Immediately:**
	  ▪ Use registered communication channels or user account.
	  ▪ Include a clear description of the breach (nature, extent, timing), likely consequences, mitigation measures, safety steps for the Data Principal, and contact details for queries.
	▪ **Notify the Data Protection Board:**
	  ▪ Provide initial description without delay (nature, extent, timing, location, impact).
	  ▪ Submit a comprehensive report within 72 hours (or an extended period if permitted), including breach details, mitigation and remedial actions, findings on the responsible party, and a report on notifications sent to affected Data Principals.

Rule 8 – Retention and Deletion	▪ **Erasure Obligation:**
	  ▪ Data Fiduciary must erase personal data after the retention period specified in the Third Schedule, unless retention is required by law.
	  ▪ Erasure applies when the Data Principal does not engage for the specified purpose or exercise rights.
	▪ **Advance Notice:**
	  ▪ Notify the Data Principal at least 48 hours prior to erasure that data will be deleted unless they log in or contact the Fiduciary.
	▪ **Retention for Logs:**
	  ▪ Retain personal data, traffic data, and processing logs for minimum one year as per the Seventh Schedule for compliance and audit purposes.
	  ▪ Erase after one year unless further retention is required by law or government notification.

Rule 9 – Display the Business Contact	▪ **Publication Requirement:** Every Data Fiduciary must prominently publish on its website or app, the contact details of DPO or a designated person who can respond on the fiduciary's behalf. ▪ **Communication Requirement:** Include these contact details in every response to a Data Principal exercising rights under the Act. ▪ **Purpose:** Ensure Data Principals can easily reach someone for queries about processing of their personal data.
Rule 10, 11 and 12 – Processing of Personal Data of Children and Person With Disability	▪ **Consent Obligation:** Obtain verifiable consent before processing data of a child or person with disability. ▪ **Children Verification:** Confirm that the parent/guardian is 18+ and can be positively identified. ▪ **Disability Verification:** Confirm that the guardian is appointed by court, designated authority, or local level committee. ▪ **Verification Methods:** Accept reliable identity details, voluntarily provided info, or virtual token from authorised entity. ▪ **Authorised Entity:** This includes government-approved issuers and Digital Locker Service Providers. ▪ **Applicable Laws:** Rights of Persons with Disabilities Act, 2016 and National Trust Act, 1999. ▪ **Person with Disability:** Individuals with long-term impairments or conditions such as autism, cerebral palsy, or severe multiple disabilities who cannot make legally binding decisions even with support. ▪ Exemption from certain obligation of the act for processing of data by certain set of data fiduciaries and for certain purpose as specified in Schedule 4.
Rule 13 – Significant Data Fiduciaries (SDF)	▪ **Annual DPIA and Audit:** Conduct DPIA and audit every 12 months. ▪ **Report Submission:** Submit DPIA and audit report with key observations to the DPB. ▪ **Technical Risk Check:** Ensure technical measures and algorithms do not risk Data Principals' rights. ▪ **Data Localization:** Restrict transfer of specified personal and traffic data outside India.
Rule 14 – Data Subject Rights	▪ **Rights of Data Principals:** Rights include access, correct, erase, and nominate; resolution within 90 days.
Rule 15 – Cross-Border Data Transfers	▪ **Transfer Allowed:** Personal data can be transferred outside India in compliance with the conditions specified by the Central Government. ▪ **Recipients Covered:** Applies when sharing data with any foreign State or its agencies, or entities under its control.
Rule 16 – Exemption for Specific Purpose	▪ Exemption from Act for research, archiving or statistical purposes if processing is in accordance with the standard specified in Second Schedule.

Minimum Security Safeguards

Data Security Measure

- Encrypt personal data during storage and transmission.
- Mask or obfuscate sensitive identifiers.
- Use of virtual tokens mapped to personal data for secure processing.

Access Control

- Restrict access to personal data based on roles and necessity.
- Ensure role-based access and multi-factor authentication to prevent unauthorized entry.

Monitoring and Detection

- Maintain detailed logs of all access to personal data.
- Enable continuous monitoring and periodic reviews to detect unauthorized access, investigate incidents, and prevent recurrence.

Business Resilience

- Maintain secure, encrypted backups of personal data and validate them periodically.
- Implement failover servers and disaster recovery plans to restore access quickly.

Logging and Audit

- Retain processing and traffic logs for at least one year.
- Ensure logs are tamper-proof and auditable.

Contractual Obligations

- Include clear security obligations and compliance requirements in contracts with Data Processors.
- Ensure processors follow equivalent security standards as the Data Fiduciary.

Exemptions Under DPDPA

Government and State Functions	Processing by the State or its instrumentalities for providing subsidies, benefits, services, certificates, licenses, or permits. Processing necessary for performing any function under law or policy in the interest of individuals.
Research, Archiving, and Statistical Purposes	Processing for research, archiving, or statistical purposes is exempt if conducted in accordance with the prescribed standards and if the personal data is not used to make decisions affecting individuals.
Certain Classes of Fiduciaries	Exemptions for clinical establishments, healthcare professionals, mental-health establishments, educational institutions, childcare centers, and associated transport providers.
Personal or Domestic Use	Processing by individuals for personal or domestic purposes is outside the scope of the Act.
Specified Purposes for Children	Activities such as creating user accounts for communication or determining real-time location for safety may be exempt when done lawfully.
National Security and Public Interest	Processing for national security, law enforcement, or public interest may be exempt under government notification.

Key Actions for Organizations

- **Understand Applicability and Scope:** Determine whether your organization qualifies as a Data Fiduciary or Significant Data Fiduciary and map obligations under the Act.
- **Establish a Governance Framework:** Define a clear governance structure for data protection. Appoint a DPO or Privacy Lead, delineate roles and responsibilities, and implement internal policies for accountability and oversight.
- **Conduct Data Mapping and Gap Assessment:** Identify and map personal data collected, stored, or shared across systems. Perform a gap analysis against DPDPA requirements to pinpoint remediation needs.
- **Update Privacy Notices and Consent Mechanisms:** Draft clear, multilingual privacy notices and deploy verifiable consent systems with easy withdrawal options.
- **Strengthen Security Safeguards:** Adopt robust technical and organizational measures such as encryption, access restrictions, and continuous monitoring. Maintain audit logs for a minimum of one year and ensure breach notifications within 72 hours as per rule 6.
- **Review and Update Third-Party Contracts:** Evaluate agreements with vendors and partners to ensure compliance with DPDPA obligations. Include clauses addressing data security, breach reporting, and lawful processing.
- **Initiate Employee Training and Awareness:** Conduct regular training to build awareness of DPDPA responsibilities, breach-response protocols, and secure data-handling practices.
- **Develop a Data Breach Response Plan:** Establish incident-response playbooks to notify affected individuals and report breaches to the Board within 72 hours.

Our Service Offerings

A&M's Privacy and Data Compliance experts advise and support leading organisations across all aspects of data compliance and privacy risk management. We help clients navigate complex local and international privacy rules and data laws, particularly in areas such as technology innovation, data strategy and digital services, including:

- **Global Privacy Programme Management:** Guiding senior management in designing, implementing, and enhancing the organisation's privacy function.
- **Privacy Strategy and Governance:** Conducting ongoing policy and regulatory horizon scanning, and designing and implementing privacy frameworks, policies and procedures.
- **Privacy Office Advisory Support (DPO as a Service):** Providing professional support to ensure effective management of privacy and personal data protection in accordance with applicable legislation and best international practices.
- **International Data Transfer Strategy Support:** Providing advisory and implementation support to identify, risk-assess and rationalise cross-border data flows in line with legal and business objectives.
- **Privacy Transaction Services:** Provide privacy due diligence support for corporate transactions, integrating data privacy functions, and aligning privacy governance with business and technology objectives.
- **Privacy Technology Advisory:** Privacy technology integration and support across a wide range of commercially available privacy tools and technologies.

References:
1. https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa?pageTitle=Digital-Personal-Data-Protection-Rules-2025

Contact Us

CHANDRA PRAKASH SURYAWANSHI
Managing Director

+91-9900020190
csuryawanshi@alvarezandmarsal.com

HARDIK GOGRI
Senior Director

+91 98925 36101
hgogri@alvarezandmarsal.com

ABOUT ALVAREZ & MARSAL

Founded in 1983, Alvarez & Marsal is a leading global professional services firm. Renowned for its leadership, action and results, Alvarez & Marsal provides advisory, business performance improvement and turnaround management services, delivering practical solutions to address clients' unique challenges. With a world-wide network of experienced operators, world-class consultants, former regulators and industry authorities, Alvarez & Marsal helps corporates, boards, private equity firms, law firms and government agencies drive transformation, mitigate risk and unlock value at every stage of growth.

To learn more, visit: **AlvarezandMarsal.com**

Follow A&M on:

ALVAREZ & MARSAL
LEADERSHIP. ACTION. RESULTS.℠