DIGITAL PERSONAL DATA PROTECTION (DPDP) RULES 2025

A Baker Tilly ASA India's Perspective

November 2025

DPDP RULES 2025 – SNEAK PEAK

bakertilly ASA

INTRODUCTION

The Digital Personal Data Protection (DPDP) Rules 2025, issued by the Government of India, give operational effect to the DPDP Act 2023 and establish a comprehensive regulatory framework for the processing of digital personal data. The Rules define clear, enforceable expectations for organisations relating to user notices, consent governance, data security, breach reporting, children's data protection, data retention, cross-border transfers, and obligations for Significant Data Fiduciaries (SDFs).

Together, the Act and the Rules create a structured, rights-based approach to personal data governance by mandating robust technical and organisational controls, transparent communication with users, and periodic compliance activities across all entities handling personal data in India.

KEY REQUIREMENTS

Clear User Notices
Organisations must issue standalone, plain-language notices specifying data categories, processing purposes, user rights, and mechanisms for consent withdrawal.

Consent & Withdrawal
Consent must be explicit, informed, and purpose-specific. Systems must maintain auditable records for all consent-related actions and offer easy mechanisms for withdrawal.

Mandatory Security Safeguards
Minimum prescribed safeguards include encryption, access management, logging, monitoring, and retention of access logs for at least one year.

Breach Reporting
All personal data breaches must be reported to impacted individuals and to the Data Protection Board (DPB) without delay, followed by a comprehensive report within 72 hours.

Retention & Deletion
Personal data and related logs must be retained for at least one year and erased once the specified processing purpose is fulfilled, unless required otherwise by law.

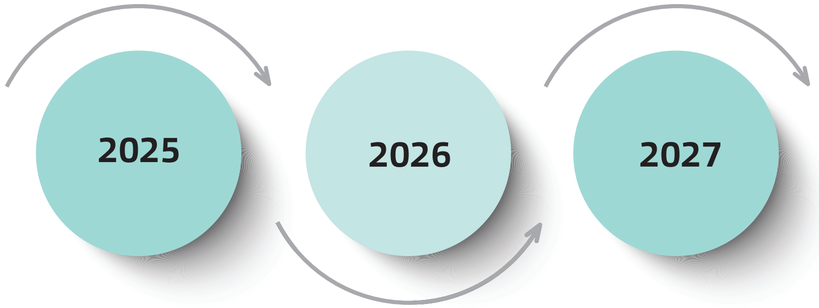
Children's Data Protection
Processing the personal data of children under 18 requires verifiable parental or guardian consent and stricter safeguards.

Significant Data Fiduciaries (SDFs)
Entities classified as SDFs must conduct annual DPIAs, independent audits, and submit compliance reports to the DPB.

Cross-Border Data Transfers
Personal data may be transferred outside India subject to government-issued conditions. SDFs may face additional restrictions on transferring specified categories of personal or traffic data

DPDP IMPLEMENTATION TIMELINE

bakertilly
ASA



Immediate (2025) – Regulatory Activation

Data Protection Board (DPB) becomes operational

Search & Selection Committees constituted

Digital Office framework launched, enabling electronic filings, hearings, notices, and compliance submissions

12 Months from Notification – Consent Ecosystem Goes Live

Consent Manager (CM) ecosystem officially operational

Registration, governance, and interoperability requirements for CMs become enforceable

Fiduciaries begin aligning consent journeys and backend systems with CM standards

18 Months from Notification – Full Compliance Window

All operational provisions of the DPDP Rules come into force

Mandatory adherence to notice, consent, security safeguards, log retention, and breach reporting requirements

Parental verification for children's data becomes enforceable

SDF obligations commence: annual DPIA, audit, algorithmic risk checks

Cross-border transfer conditions and any Government restrictions become binding

FRAMEWORK OBJECTIVES

bakertilly
ASA

APPLICABILITY

Data Fiduciaries (All Businesses Processing Personal Data)	Data Processors & Sub-Processors	Government Departments & Public Authorities	Financial Institutions & Regulated Entitie
Significant Data Fiduciaries (SDFs)	Consent Managers	Digital Platforms (E-commerce, Social Media, Gaming)	Technology & Cloud Service Providers

KEY STAKEHOLDERS IMPACTED

- Board of Directors
- Senior Management & CXOs
- Data Protection Officer (DPO) / CISO
- Business & Application Owners

The DPDP Rules apply across all organisations handling digital personal data—impacting governance, operations, technology, and compliance functions. They mandate coordinated oversight between leadership, DPOs, CISOs, and functional owners to ensure enterprise-wide data protection readiness.

WHAT DPDP RULES OUTLINE

bakertilly
ASA

Standalone, Itemised Consent Notices

Mandatory clear, purpose-specific consent notices presented independently from other terms.

Simplified Consent Withdrawal

Every fiduciary must provide frictionless, comparable mechanisms for withdrawing consent.

Mandatory Log & Data Retention (1 Year Minimum)

Access logs, traffic data, and relevant records must be retained for at least one year.

Time-Bound Breach Reporting

Data breaches must be reported without delay to the DPB and affected individuals, followed by a detailed report within 72 hours.

Annual SDF Compliance Requirements

Significant Data Fiduciaries must conduct annual DPIAs, independent audits, and submit compliance reports.

Children's Data: Verifiable Parental Consent

New verification requirements introduced to confirm the identity and majority of parents/guardians before processing children's data.

Cross-Border Transfer Conditions

Data transfers outside India are permitted but remain subject to future government-notified restrictions or negative lists.

Expanded Government Powers

Government agencies may seek information for defined public-interest purposes and can prohibit disclosure that such requests were made.

DPDP RULES 2025: THE THREE PILLARS OF INDIA'S NEW DATA PROTECTION FRAMEWORK

bakertilly ASA

User Trust & Consent Governance

Empowering Data Principals through transparent, granular, and easy-to-manage consent mechanisms. Organisations must adopt plain-language notices, itemised purpose specification, accessible withdrawal options, and lifecycle-based data minimisation practices including timely erasure and inactive-user governance.

Security & Incident Readiness

Strengthening operational resilience through mandated technical and organisational controls. The Rules define minimum safeguards such as encryption, access management, and one-year log retention. Breach reporting to both the DPB and affected individuals is required, with a strict 72-hour reporting window.

Governance & Accountability

Elevating oversight and responsibility across high-impact data environments. Significant Data Fiduciaries must appoint a DPO, conduct annual DPIAs and audits, validate algorithmic systems, and maintain robust grievance redressal processes—all supported by a penalty framework that enforces compliance discipline.

A Unified Framework Strengthening Trust, Security, and Accountability

The Digital Personal Data Protection (DPDP) Rules 2025, notified under the DPDP Act 2023, establish a comprehensive and enforceable framework for responsible handling of personal data in India.They position data protection as a strategic business priority—strengthening user trust, enabling operational resilience, and reducing regulatory and reputational risk.

PILLAR 1: THE TRUST MANDATE –
USER CONTROL & TRANSPARENT CONSENT

bakertilly
ASA

WHY THIS PILLAR MATTERS

This pillar defines how organisations communicate with users, collect consent, and manage data transparency. It shifts compliance from a legal formality to a trust-building design principle.

KEY REQUIREMENTS

1. **Clear & Plain-Language Notices (Rule 3)**
   - Standalone, concise notices explaining data categories and processing purposes.
   - No bundled or buried disclosures inside Terms of Service.
2. **Itemised & Purpose-Specific Consent**
   - Each purpose must be clearly defined and separately indicated.
   - Generic “marketing” or “service improvement” consent is no longer sufficient
3. **Easy & Comparable Withdrawal Mechanisms**
   - Opt-out must be as simple and accessible as opt-in.
   - Full audit trails of consent and withdrawal must be maintained.

Data Lifecycle Responsibilities

4. **Mandatory Data Erasure (Rule 8)**
   - Data must be deleted once the purpose has been fulfilled.
   - Enforces “data minimisation by design.”
5. **Inactive User Policy**
   - Users identified as inactive must be notified 48 hours before deletion.
   - Any interaction resets the clock.

PILLAR 2: OPERATIONAL IMPERATIVE – SECURITY & CRISIS MANAGEMENT

bakertilly ASA

PURPOSE OF THIS PILLAR

Ensures that organisations implement robust technical safeguards and have the ability to respond rapidly to breaches and security incidents.

CORE SECURITY CONTROLS (RULE 6)

1. **Encryption & Obfuscation**
   - Protect data at rest and in transit using industry-grade technologies.
2. **Access Control & Authorisation**
   - Role-based access, privileged access policies, and monitoring.
3. **Logging, Monitoring & Retention**
   - Maintain comprehensive logs for minimum one year.
   - Support forensic investigations, audit reviews, and regulatory inquiries.

Breach Response Requirements (Rule 7)

4. **Notification to the Data Protection Board (DPB)**
   - Report breaches without undue delay.
   - Submit a detailed incident report within 72 hours.
5. **Notification to Data Principals (Users)**
   - Mandatory disclosure of impact, risk, and recommended mitigation actions.

Organisational Readiness

6. **Crisis response teams, playbooks, and escalation protocols must be in place.**

PILLAR 3: GOVERNANCE & RISK – ACCOUNTABILITY FRAMEWORK

bakertilly ASA

PURPOSE OF THIS PILLAR

Establishes a structured, risk-based governance model with heightened duties for Significant Data Fiduciaries (SDFs).

OBLIGATIONS FOR SIGNIFICANT DATA FIDUCIARIES (RULE 13)

1. **Appoint a Data Protection Officer (DPO)**
   - Must be based in India.
   - Acts as the primary liaison for the DPB and Data Principals.
2. **Mandatory Annual Assessments**
   - Data Protection Impact Assessment (DPIA).
   - Independent data protection audit.
   - Reports must be submitted to the Board.
3. **Algorithmic Due Diligence**
   - Ensure automated or AI-driven processing does not cause harm or bias.
   - Enhanced oversight for profiling and automated decision-making.

Grievance & Redressal (Rule 14)

4. **Robust User Complaint Management**
   - All grievances must be resolved within 90 days.
   - Requires defined workflows and ownership across business units.

Penalty Exposure

5. **Financial Penalties for Non-Compliance**
   - Breach notification failures may attract penalties up to ₹200 crore.
   - Reinforces data protection as a critical business risk.

KEY AREAS WHERE RULES HAVE RESERVED THE ROOM FOR FUTURE AMMENDMENTS

bakertilly
ASA

SDF Classification

Criteria relating to data volume, sensitivity levels, and risk factors are yet to be notified. This impacts whether organisations must appoint a DPO, conduct annual audits, and perform DPIAs.

Security Safeguards

The Rules describe baseline safeguards but do not define expected maturity or mapping to global frameworks, leading to interpretive variance on “reasonable security.”

Cross-Border Transfers

The Government’s negative-list of restricted jurisdictions is awaited. This limits clarity on cloud hosting, offshore processing, and global data infrastructure planning.

Children’s Data & Parental Consent

No prescribed model for verifying parental or guardian consent has been issued.Businesses must design their own systems, increasing cost and compliance fragmentation.

Processor Responsibilities

Obligations focus primarily on Data Fiduciaries. Direct accountability expectations for Data Processors remain limited, leaving gaps in contractual alignment and oversight.

Right to Erasure & Inactivity Reset

The reset mechanism for inactive accounts may dilute the user’s deletion rights.Clarification is needed on how platforms with high engagement should operationalise erasure.

About us

bakertilly
ASA

A full service Accounting & Consulting Firm

SERVICES

- Accounting and Business Support
- Assurance
- Business Advisory
- Cyber Security
- Global Offshoring Services
- Risk Advisory
- Taxation
- Transaction Advisory

PRESENTLY POSITIONED IN THE

TOP 10 ACCOUNTING & CONSULTING FIRMS

Well structured teams with domain specialization are guided by leaders who possess expertise and experience and are present PAN India to ensure excellent client service.

19 Locations

70 Partners/ Directors

6000+ Clients

1300+ In-house Professionals

GLOBAL PRESENCE

43,000 Staff

700 Offices

$5.6bn Turnover

143 Territories