A Detailed Breakdown of
India's DPDP Rules, 2025:
What Every Organisation Must Know

India's **Digital Personal Data Protection Rules, 2025,** bring operational clarity to the DPDP Act, 2023, and formally define how organisations must collect, store, process, protect, transfer, and delete personal data. These rules impose strict technical, legal, and governance duties on Data Fiduciaries, Data Processors, and Consent Managers.

Below is a **point-wise breakdown with detailed explanations,** referencing the **specific Rules** wherever applicable.

Definition of User Account, Verifiable Consent, Techno-Legal Measures (Rule 2)

Rule 2 clarifies several key terms that appear repeatedly throughout the Rules.

Description

A ***User Account*** refers to any identity created to access a service—email ID, username, mobile number, or any identifier.

Verifiable Consent is defined as consent that satisfies Rules 10 and 11, particularly for children and persons with disabilities.

Techno-Legal Measures refer to structured technical and legal safeguards referenced under Rules 20 and 22, forming the backbone of the governance framework.

These definitions remove ambiguity and guide the interpretation of all responsibilities under the DPDP framework

---

Notice Requirements for Collecting Personal Data (Rule 3)

Rule 3 establishes the standard of transparency that Data Fiduciaries must meet before collecting personal data.

Description

The notice must be ***independent, plain-language,*** and clearly describe the personal data being collected.

Rule 3(1)(a) specifically requires an ***itemised list*** of personal data categories.
Rule 3(1)(b) mandates a specific ***purpose description,*** not generic statements.
Rule 3(1)(c) requires a ***direct link*** for Data Principals to withdraw consent, exercise rights, or lodge complaints.

This transforms the communication model from *"hidden terms"* to clear, user-centric transparency.

Duties of Consent Managers (Rule 4 + First Schedule)

Consent Managers are central to India's privacy architecture.

Description

Rule 4 requires Consent Managers to register with the Government one year after the Rules come into force.

The First Schedule (Part A) prescribes criteria for registration—such as being an Indian-incorporated company, maintaining a minimum ₹2 crore net worth, and having adequate technical and organisational capacity.

Part B details obligations: a Consent Manager must enable individuals to give, manage, and withdraw consent; must maintain consent records for seven years; must ensure data shared through them is unreadable; and must avoid conflicts of interest.

This creates an independent, auditable ecosystem for consent governance.

Reasonable Security Safeguards (Rule 6)

Rule 6 lists mandatory baseline cybersecurity practices every organisation must follow.

Description

Organisations must use ***encryption, masking, pseudonymisation, or tokenisation*** to protect personal data.

They must implement ***access controls*** to restrict who can access what data.

Rule 6(2) requires ***logging, monitoring, and periodic review*** of access events.
Rule 6(3) demands robust ***data backup*** mechanisms.
Rule 6(4) states that logs and personal data must be retained for ***one year*** even if users request deletion.

Rule 6 ensures that security becomes a legally mandated priority, not an optional one.

Breach Notification Requirements (Rule 7)

Rule 7 prescribes the timeline and content of mandatory breach notifications.

Description

Organisations must notify both the ***affected Data Principals*** and the ***Data Protection Board "immediately"*** after detecting a personal data breach.

The notification to Data Principals must include the ***nature of the breach, consequences, mitigation steps,*** and ***contact details of the responsible officer.***

A detailed report must be submitted to the Board ***within 72 hours,*** explaining the circumstances, cause of breach, corrective actions, and confirmation of user notifications.

India now aligns with global standards like GDPR's 72-hour reporting rule.

Data Retention, Purpose Limitation & Mandatory Erasure (Rule 8 + Third Schedule)

Rule 8 fundamentally changes how long businesses may retain data.

Description

Under Rule 8(1), personal data must be erased when the "specified purpose is no longer served.

The ***Third Schedule*** identifies organisations, such as e-commerce platforms, online gaming intermediaries, and social media platforms, that must erase data if users do not return to the service for a defined period.

Rule 8(2) requires organisations to give ***48 hours' prior notice*** before erasing a user's data.
Rule 8(5) states that logs must still be retained for ***one year*** even after erasure.

This eliminates indefinite data retention and forces lifecycle-based data governance.

Data Audits & Additional Obligations for Significant Data Fiduciaries (Rule 9)

Rule 9 introduces enhanced obligations for organisations classified as Significant Data Fiduciaries.

Description

Such organisations must conduct ***Data Protection Impact Assessments (DPIAs),*** periodic compliance audits, and appoint a ***Data Protection Officer (DPO)*** at a senior level. They must also implement stricter monitoring, governance, and reporting mechanisms.

This rule ensures high-risk processing environments maintain heightened accountability.

Processing of Children's Data(Rule 10)

Rule 10 introduces strict requirements for children's privacy.

Description

Data Fiduciaries must obtain ***verifiable parental consent*** before processing personal data of children.

Verification must rely on ***"reliable government-issued identity proof,"*** virtual tokens approved by the Government, or Digital Locker-based verification. Platforms must ensure that parental consent is legitimate and not easily spoofed.

This rule prevents unauthorised or harmful processing of children's data.

Consent for Persons with Disabilities (Rule 11)

Rule 11 extends protections to individuals who require lawful guardians.

Description

Consent must be obtained from a ***verified lawful guardian,*** and the Data Fiduciary must validate such guardianship under the provisions of Indian laws including the ***Rights of Persons with Disabilities Act, 2016*** and the ***National Trust Act, 1999.***

Data Principal Rights & Complaint Handling (Rule 14)

Rule 14 outlines the mechanisms for Data Fiduciaries to enable user rights.

Description

Organisations must clearly communicate how Data Principals can exercise rights under the Act, such as access, correction, erasure, grievance redressal, and nomination. A grievance officer must respond within 90 days. Organisations must explain what identifiers users need to provide to authenticate rights requests.

Rule 14 ensures user empowerment is practical, not just theoretical.

Cross-Border Data Transfer (Rule 15)

India adopts a flexible approach to international data flows.

Description

Rule 15 states that personal data may be transferred outside India ***unless*** the Central Government restricts certain countries or territories. This mirrors global frameworks where the Government exercises oversight while enabling international business operations.

Consent Revocation & Restrictions on Dark Patterns (Rule 16)

Rule 16 ensures consent withdrawal is smooth and user-friendly.

Description

Organisations must provide a ***simple, accessible, and transparent mechanism*** for consent revocation. This mechanism must be as simple as giving consent, ensuring no dark patterns or manipulative interface designs.

Governance Framework for Technical Standards (Rule 20–22)

These rules define how techno-legal standards will be enforced.

Description

Rule 20 discusses Government-prescribed technical standards for secure processing.
Rule 21 deals with transparency requirements for algorithms if used in automated decision-making.
Rule 22 defines data-sharing formats, interoperability guidelines, and record maintenance systems.

This ensures India's digital ecosystem becomes standardised and auditable.

Government Access & Exemptions (Rule 23 + Second & Seventh Schedules)

Rule 23 outlines circumstances under which Government agencies may demand information.

Description

Government bodies may request data for purposes listed in the ***Seventh Schedule,*** including national security, regulatory compliance, and legal enforcement. In specific cases, organisations may be directed ***not to inform*** the Data Principal about such requests.

The ***Second Schedule*** permits exemptions for research, archiving, and statistical analysis, subject to strict behavioural standards.
This balances privacy with lawful public interest.

Closing Remarks

The DPDP Rules, 2025 redefine the way Indian organisations must manage personal data. They introduce transparent notice requirements, strict consent governance, mandatory security safeguards, breach-reporting duties, data retention limits, and enhanced protections for children and persons with disabilities.

With clear rule-by-rule obligations, the Rules require organisations to overhaul their governance models, technical architecture, and user-facing processes. Early compliance will not only minimise regulatory risk but also build trust with customers in an increasingly privacy-conscious digital world.

Source:

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

Want to implement the DPDP Act in your organization?

Contact Us At

sales@kratikal.com
+91 9289192210
www.kratikal.com