Digital Personal Data Protection Rules, 2025

(Based on the official MeitY-notified DPDP Rules, 2025)

The Digital Personal Data Protection Rules, 2025 were introduced by the Ministry of Electronics and Information Technology on 14 November 2025 to formally operationalise the Digital Personal Data Protection Act, 2023. These Rules set the practical framework for how organisations in India must collect, process, store, secure, and delete personal data. They exist to bring consistency, transparency, and accountability to data handling practices across sectors. By clearly defining consent requirements, security standards, user rights, data retention norms, and governance expectations, the Rules ensure that personal data is managed responsibly and that digital businesses operate within a unified and enforceable privacy regime.

Rule 1 — Short Title and Commencement

This rule states:

- The name of the rules is **Digital Personal Data Protection Rules, 2025**.
- Certain rules take effect immediately on publication in the Official Gazette.
- Other rules take effect on dates specified later by the Government.

Meaning: Some obligations start immediately. Others will activate in phases (12 months, 18 months, or as notified).

Rule 2 — Definitions

This rule defines key terms used throughout the Rules such as:

Data Fiduciary

The entity deciding why and how data is processed

Data Principal

The individual whose data is processed

Consent

Agreement for data processing

Personal data

Information relating to an individual

Board

Data Protection Board of India

Meaning: The definitions in these Rules supplement the definitions under the DPDP Act, 2023 and ensure consistent interpretation.

Rule 3 — Form and Content of Privacy Notice

A Data Fiduciary must give a **standalone**, **clear**, and **plain-language** notice to the Data Principal before collecting personal data. This notice must include:

- Categories of personal data being collected
- Purpose of processing
- How long the data will be retained
- How the individual can exercise rights
- How consent may be withdrawn
- Whether the data will be shared, and with whom
- How the Data Principal may lodge grievances or complaints
- Details of Data Protection Officer or grievance officer where applicable

Meaning: No bundled, vague, or hidden notices. The notice must be easily understandable and transparent.

Rule 4 — Consent Requirements

This rule explains how valid consent must be obtained. Consent must be:

Free

Given without coercion or pressure

Informed

Based on clear understanding

Specific

For particular purposes

Unambiguous

Clear and explicit agreement

Withdrawable

As easily as it was given

The Data Fiduciary must maintain records of consent.

Meaning: Consent cannot be bundled with terms and conditions, forced, or implied.

Rule 5 — Security Safeguards

Data Fiduciaries must implement "reasonable" **technical and organisational measures**, including:

- Encryption or equivalent protection
- Access controls
- Identity verification controls
- Activity logs
- System monitoring
- Periodic reviews of internal practices
- Vendor and processor security checks

Meaning: Security must be in line with risk and industry standards. Organisations must document and demonstrate these safeguards when needed.

Rule 6 — Data Breach Notification

If there is a personal data breach, the Data Fiduciary must:

Notify the Data Protection Board

Immediately in the manner prescribed

Notify all affected Data Principals

With full details of the breach

The notification to Data Principals must explain:

- What happened
- What personal data was involved
- Likely risks or harm
- Steps the Data Principal must take
- Measures the Data Fiduciary is taking

The Data Fiduciary must retain breach-related logs for the period specified.

Meaning: Breach reporting is mandatory, fast, and transparent.

Rule 7 — Data Principal Rights Execution

Data Fiduciaries must set up easy-to-use systems for individuals to:

Access their own data

Request correction

Request completion or updating

Request deletion

Withdraw consent

Acknowledge and act on these rights within prescribed timelines.

Meaning: You must have functional internal processes for responding to user rights.

Rule 8 — Data Retention and Erasure

> Personal data can be retained only as long as necessary for the purpose stated.

> Once the purpose is complete, the data must be **deleted**, unless retention is legally required.

> For data inactive for a defined period, the Data Fiduciary must issue a notice before deletion.

Meaning: No "store forever" policies. Clear retention schedules are mandatory.

Rule 9 — Processing of Personal Data of Children

Below 18 years

Age threshold for child protection

- Verifiable parental consent must be obtained before processing a child's data.
- Data Fiduciaries must verify that the consenting person is the parent/guardian.
- Behavioural monitoring or targeted advertising to children is restricted.

Meaning: Strict child safety and parental-consent mechanisms are required.

Rule 10 — Additional Safeguards for Persons with Disabilities

Guardian Representation

A lawful guardian or authorised person may act on behalf of the individual.

Accessibility Requirements

Data Fiduciaries must ensure accessibility for persons with disabilities.

Meaning: Rights must be accessible to vulnerable individuals.

Rule 11 — Exemptions for Research, Archival and Statistical Purposes

Certain kinds of processing may be exempt if:

- Personal data is anonymised or de-identified
- The purpose is statistical, research-oriented, or archival
- Results are not used to make decisions about individuals

Meaning: Research/analytics use cases get conditional exemptions.

Rule 12 — Cross-Border Data Transfer

Default Permission

Personal data may be transferred outside India unless restricted by the Central Government for specific countries or classes.

Ongoing Responsibility

Data Fiduciaries remain responsible for protection even after transfer.

Adequate Safeguards

Adequate safeguards must be ensured.

Meaning: Default open, but subject to future government restrictions.

Rule 13 — Classification and Obligations of Significant Data Fiduciaries (SDFs)

SDFs are identified based on:

- Volume of data processed
- Sensitivity
- Risk to rights
- Impact on national interests

SDF obligations include:

1. Mandatory Data Protection Officer
2. Annual Independent Audits
3. Data Protection Impact Assessments
4. Algorithmic assessments where relevant
5. Higher standards of governance and accountability

Meaning: Large or high-risk companies must follow stricter rules.

Rule 14 — Consent Managers

Registration

Consent Managers must register with the Government.

Platform Requirements

They must offer interoperable, secure, user-friendly platforms.

User Control

Users can give, manage, or withdraw consent through them.

Meaning: A regulated, standardised consent-management ecosystem.

Rule 15 — Grievance Redressal Requirements

Data Fiduciaries must:

Enable Complaints Enable Data Principals to lodge complaints	**Provide Contact Details** Provide contact details of officers
Respond Promptly Respond within fixed timelines	**Maintain Records** Maintain records of grievances

Meaning: Fast and formal grievance mechanisms are mandatory.

Rule 16 — Duties of Data Principals

This rule reminds individuals of their duties, such as:

- → Not providing false information
- → Not filing false grievances
- → Providing accurate identification documents where required

Meaning: Individuals also have responsibilities.

Rule 17 — Appointment and Functioning of the Data Protection Board

This rule outlines how the Board will be set up:

- Composition, appointments, terms of service
- Functions, powers, inquiry procedures
- Manner of issuing orders and penalties

Meaning: The Board is the regulatory enforcement body.

Rule 18 — Penalties and Enforcement Procedures

Specifies:

- How penalties will be calculated
- What factors the Board considers
- Procedure for hearings
- Opportunity to be heard
- Timeline for compliance directions

Meaning: Clear enforcement and penalty structure.

Rule 19 — Reporting, Audits, and Record-Keeping

Data Fiduciaries must maintain:

- Records of processing activities
- Security measures
- Breach records
- Consent logs
- Audit reports (mandatory for SDFs)

Meaning: Documentation is essential for compliance.

Rule 20–23 — Miscellaneous Provisions

Includes:

- Transitional arrangements
- Repeals/overriding effect
- Power of Central Government to issue further directions
- Future rule-making provisions

Meaning: Gives flexibility for future amendments and clarifications.

IMMEDIATE vs LATER Implementation (Final Summary)

Immediately Required

(Note that DPDPA's administrative machinery has been operationalised, its substantive impact will materialise only once the rest of the Act is enforced.)

- Start using compliant privacy notices
- Start using valid consent collection
- Implement basic security safeguards
- Prepare breach detection and notification mechanism
- Start mapping data, retention periods, deletion flows
- Make user rights accessible
- Basic governance alignment to DPDP Act and Rules

Within 12 Months

- Consent Manager registration (for companies acting as Consent Managers)
- Framework for parental-verification systems
- Initial data protection governance structures

Within 18 Months

- Full operational roll-out of notice and consent frameworks
- Full security controls
- Mandatory breach notifications
- Full children's data compliance
- DPIAs, audits, algorithmic assessments for SDFs
- Cross-border transfer compliance structures

Key Takeaways / Some points of caution

- The Rules introduce an 18-month transition in many parts, but the faster you act the better — compliance lag may become a liability.
- The interpretation/application of some terms (what qualifies as "Significant Data Fiduciary", what counts as "sensitive categories" for localization) may be refined later — staying up to date is key.
- For cross-border transfers: while permitted, some categories may get localization restrictions in future. So if your services involve data storage overseas, monitor that.
- The government may shorten compliance deadlines, per recent statements.
- Marketing / content claims should be accurate: If you state "we are DPDP-compliant", ensure you actually are—not just in plan stage.

HEDGE-SQUARE
Beyond Consultancy

Contact Us

contact@hedge-square.in

+91 8692 0516 11

https://hedge-square.com/