CORRIDALEGAL
Corporate & Employment Law Firm

Primer On

The Digital Personal Data Protection Rules, 2025

WWW.CORRIDALEGAL.COM

Re: Handbook On Primer On Digital Personal Data Protection Rules, 2025: Rules Explained

Date: _____

For: Client's Legal, IT Security and HR Teams

INDEX

01

ABOUT US

INDIA'S MOST TRUSTED CORPORATE & EMPLOYMENT LAW SPECIALISTS: WE CARE

We are a boutique corporate & employment law firm serving as strategic partners to businesses by helping them navigate transactions, fundraising-investor readiness, operational contracts, workforce management, data privacy and disputes. We keep our clients' future ready by ensuring compliance with the upcoming Indian Labour codes on Wages, Industrial Relations, Social Security, Occupational Safety, Health, Working Conditions and the Digital Personal Data Protection Act, 2023. With offices across India, including Delhi, Mumbai and Gurgaon, coupled with global partnerships with international law firms in Dubai, Singapore, the United Kingdom and the USA, we are the preferred law firm for India entry and international business setups.

I. Introduction

The Digital Personal Data Protection Act, 2023 ("DPDP Act") laid the foundation for a modern data protection regime in India. With the notification of the Digital Personal Data Protection Rules, 2025 ("DPDP Rules"), the statutory framework is now operational.

The DPDP Rules translate the DPDP Act's principles into a practical compliance system. Developed through wide consultation across major cities and sectors, the DPDP Rules emphasise simplicity, accountability and citizen empowerment. They also reflect the SARAL (Simple, Accessible, Rational and Actionable) philosophy, to ensure clarity for both individuals and organisations. This primer provides a structured and practical overview of the DPDP Rules, 2025.

II. Overview of the DPDP Rules, 2025

The Rules flesh out key areas such as:

1. Form and content of consent notices
2. Obligations for Consent Managers
3. Security safeguards
4. Data breach reporting requirements
5. Retention standards and deletion obligations
6. Special protections for children and persons with disabilities
7. Rights of Data Principals and grievance timelines
8. Obligations of Significant Data Fiduciaries ("SDFs")
9. Conditions for cross-border transfers
10. Functioning of the Data Protection Board of India ("DPB")
11. Procedures for filing appeals

The framework balances privacy protection with innovation-friendly compliance, especially for startups and MSMEs.

III. Effective Dates and Phased Implementation

The Rules adopt a three-stage operational timeline:

Immediately Effective:
Rules 1, 2 and 17–21 (definitions and establishment of the Data Protection Board).

Effective One Year After Notification:
Rule 4 (registration of Consent Managers).

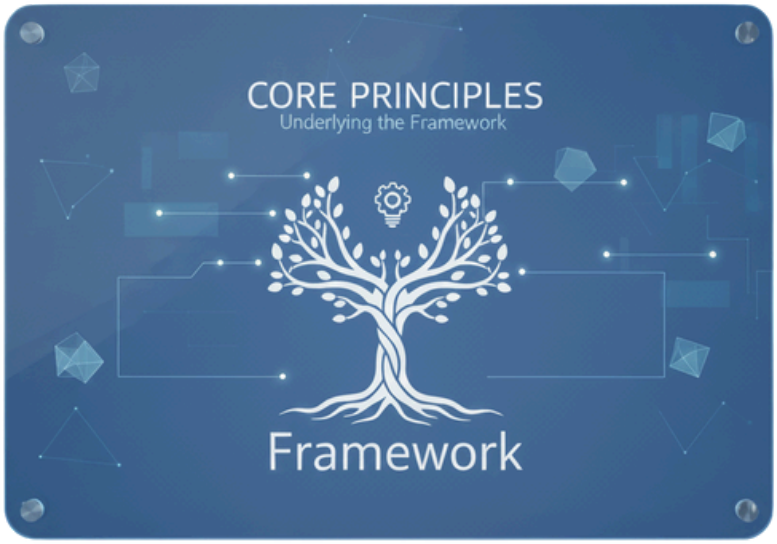
Effective Eighteen Months After Notification:
Rules 3, 5–16, 22 and 23 (core obligations including notice, consent, security safeguards, data breach reporting, rights of Data Principals and appeals).

IV. Core Principles Underlying the Framework

The Rules continue the Act's emphasis on:

- Transparency of processing
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Security safeguards
- Accountability of Data Fiduciaries

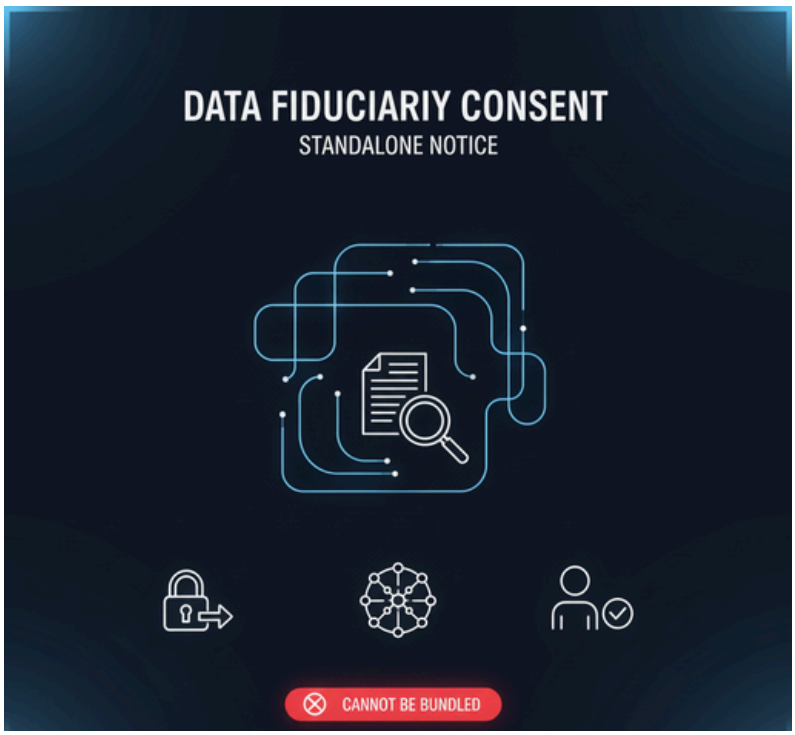
These principles guide every operational requirement.



V. Notices and Conditions for Consent (Rule 3)

Rule 3 mandates that a Data Fiduciary seeking consent must issue a standalone notice that is clear and accessible. The notice must:

- itemise the personal data proposed to be collected;
- specify each purpose of processing and identify the goods or services for which data is required;
- provide a communication link to its website/app explaining how rights may be exercised;
- describe all available methods for withdrawing consent and ensure withdrawal is no more difficult than giving consent; and
- include the business contact information of the appropriate officer.



The notice cannot be bundled with unrelated information.

VI. Consent Managers – Eligibility and Duties (Rule 4 & Schedule I)

Only Indian-incorporated companies may register as Consent Managers. To be eligible, an applicant must demonstrate:

- Minimum net worth of Rs. 2 crore;
- Adequate technical, financial and organisational capacity;
- Management personnel with a reputation for integrity; and
- An interoperable platform independently certified for compliance with Board-issued standards

Once registered, a Consent Manager must:

- keep all personal data processed through its systems unreadable to itself;
- maintain detailed and tamper-proof consent logs;
- avoid conflicts of interest with Data Fiduciaries;
- refrain from subcontracting statutory functions;
- operate a consistent user interface (website or app); and
- implement and maintain strong security safeguards.

Its role is fiduciary in nature, requiring prioritisation of Data Principals' interests.

VII. Processing Without Consent – Notice Requirements (Rule 6)

Where personal data is processed without consent under Section 7(b) of the Act, the Data Fiduciary must issue a specific notice containing:

- the business contact details of the authorised person;
- a communication link to its website/app for exercising rights; and
- all disclosures required by government-issued standards.

This ensures transparency even where consent is not the legal basis of processing.

VIII. Reasonable Security Safeguards (Rule 5)

Every Data Fiduciary must implement safeguards that include:

- Encryption, masking, obfuscation or tokenisation;
- Access-control mechanisms;
- Logging and monitoring of access to detect unauthorised activity;
- Measures to ensure continuity of processing in case of compromise;
- Contractual obligations requiring Data Processors to adopt equivalent safeguards; and

- Technical and organisational measures to keep security practices current.

These requirements reduce the likelihood and impact of personal data breaches.

IX. Personal Data Breach Notification Protocols (Rule 7)

A Data Fiduciary must notify both:

Each affected Data Principal

The Data Protection Board

without delay upon becoming aware of a personal data breach. The notice to the Data Principal must be in plain language and include:

- Nature, extent and timing of the breach;
- Likely consequences;
- Remedial actions already taken;
- Steps the individual should take; and
- Contact details of a responsible officer.

Within 72 hours of notifying the Board, the Data Fiduciary must provide:

- Updated breach details;
- Causes and circumstances;
- Mitigation measures;
- Findings on individuals involved;
- Actions taken to prevent recurrence; and
- Confirmation of notice sent to affected individuals.

X. Data Retention, Deletion and Advance Notice (Rule 8 & Schedule III)

Rule 8 introduces uniform standards for retention and deletion.

A. Mandatory Deletion

Data Fiduciaries specified in Schedule III (e-commerce platforms with 2+ crore users, certain social media intermediaries, large gaming platforms) must delete personal data if:

- the Data Principal has remained inactive for the period specified in Schedule III; and
- no law requires continued retention.

B. Advance Notice

Data Principals must receive 48 hours' notice before the scheduled deletion, informing that the data will be permanently erased unless the individual logs in or exercises her rights.

C. Minimum One-Year Retention

All Data Fiduciaries must retain processing logs and related records for at least one year for purposes listed in Schedule VII, including audits, legal inquiries and law-enforcement needs.

XI. Contact Details of Data Fiduciaries (Rule 9)

Each Data Fiduciary must prominently display on its website/app:

- Business contact details of its Data Protection Officer; or
- Another authorised person is able to respond to queries.

These details must accompany every rights-related communication.

XII. Processing of Children's Data (Rule 10 & Schedule IV)

Processing children's personal data requires verifiable parental consent. Verification may rely on:

- Existing identity information; or
- Identity/age details voluntarily provided by the parent, including through virtual tokens.

Exemptions

Schedule IV provides limited exemptions for:

Clinical establishments and healthcare professionals

Allied health practitioners

These apply only where processing directly relates to healthcare, education or real-time safety.

XIII. Data of Persons with Disabilities (Rule 11)

If a person with a disability cannot provide consent independently even with support, consent must be obtained from a lawful guardian whose authority must be duly verified.

XIV. Additional Obligations for Significant Data Fiduciaries (Rule 13)

SDFs must:

- conduct annual Data Protection Impact Assessments (DPIAs);
- undergo independent annual data audits, with significant findings submitted directly to the Board;
- ensure technical systems deployed do not compromise Data Principals' rights; and
- comply with Government-notified restrictions on transfer of specified data categories, including localisation requirements.

XV. Additional Obligations for Significant Data Fiduciaries (Rule 13)

Data Fiduciaries must clearly publish on their website/app:

- How Data Principals may exercise rights of access, correction, updating and erasure;
- Methods for submitting requests; and
- Identifiers required for verification (such as customer IDs, mobile numbers, licence numbers).

A grievance redress system must be operational within 90 days. Data Principals may also nominate another person to exercise rights on their behalf.

XVI. Additional Obligations for Significant Data Fiduciaries (Rule 13)

Data Fiduciaries may transfer personal data outside India subject to:

Government-notified conditions or

Restrictions applicable to foreign States or entities controlled by them.

XVII. Exemptions for Research, Archiving and Statistical Purposes (Rule 16)

Processing for research, archival or statistical purposes is exempt if carried out in accordance with the safeguards specified in Schedule II.

XVIII. Data Protection Board of India (Rules 17–21)

The Board will function entirely through digital platforms enabling online filing, tracking and communication. Its responsibilities include:

- Monitoring compliance with the Act and Rules;
- Determining penalties;
- Directing remedial measures; and
- Facilitating technology-driven dispute resolution.

Staffing, procedures and other administrative matters are also covered under these Rules.

XIX. Appeals Before the Appellate Tribunal (Rule 22)

Aggrieved persons may file digital appeals before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT). The Tribunal may regulate its own procedure and is not bound by the Code of Civil Procedure.

XX. Authorised Officers and Techno-Legal Measures (Rule 23)

Rule 23 identifies authorised officers empowered to issue directions or perform functions under the Rules. The definition of techno-legal measures covers standards prescribed in Rules 20 and 22, including:

- Technical controls;
- Machine-verifiable compliance mechanisms; and
- Digital document handling and authentication standards.

XXI. Key Schedules to the Rules

- **Schedule II**
  Safeguards for research, statistical and archival processing.
- **Schedule III**
  Mandatory retention periods for large digital platforms.
- **Schedule IV**
  Categories of Data Fiduciaries exempt from child-related processing restrictions.
- **Schedule VII**
  Purposes for which minimum one-year retention is required.

XXII. Conclusion

The DPDP Rules, 2025 complete India's transition from a principle-based privacy law to a fully operational compliance regime. Organisations must now align their practices, systems and policies with the detailed standards set out in the Act and Rules.

With structured transition timelines and technology-neutral requirements, the framework enables responsible innovation while safeguarding the rights of individuals.

Thank You

Contact Us

Phone
+91-9211410147

Email
contact@corridalegal.com

Website
www.corridalegal.com

Addres
Gurgaon-New Delhi-Mumbai