The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

Digital Personal Data Protection Rules, 2025: Operationalizing India's Data Privacy Framework

- ***Nagashree R***

Introduction

The Digital Personal Data Protection (DPDP) Rules, 2025, notified by the Ministry of Electronics and Information Technology (MeitY) on November 13, 2025 (published as G.S.R. 846(E)),[1] signify a historic advancement in India's electronic administration. Such regulations offer the elaborate functional structure to execute the Digital Personal Data Protection Act, 2023 (DPDP Act), that was enacted on August 11, 2023. Collectively, they set up a complete. People focused system for the handling of electronic individual information, harmonizing personal confidentiality entitlements with the requirements of legal legitimate information utilization by entities.

The rules were completed subsequent to comprehensive general feedback. The preliminary version was issued on January 3, 2025, seeking opinions up to 18, 2025, succeeded by countrywide interested party deliberations in various urban centers. More than 6,915 submissions from emerging business, MSMEs, sectors associations, public community, and residents influenced the ultimate edition.

Background and Objectives

The DPDP Act, 2023,arose as India's initial complete broad based data protection law, influenced by worldwide benchmarks whilst embracing a 'SATAL' (Simple, Accessible, Rational, and Actionable)[2] approach with plain language and examples. It extends to the handling of electronic individual information inside India and, in specific instances, to handling beyond India if it entails providing items or facilities to parsons in India.

The 2025 Rules implement essential clauses by detailing mandates for notification, approval, safety measures, violation notification, information preservation, duties of major information custodians (SDFs),[3] safeguards for minors and individuals with impairments, an the operations of the Data Protection Board of India (DPB)

---

[1] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (Nov. 13, 2025) (India).

[2] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 1 (Aug. 11, 2023).

[3] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), pmbl. (Nov. 13, 2025) (referring to draft notification G.S.R. 02(E), Jan. 3, 2025).

Primary objectives include:

1. Empowering Data Principles (individuals) with enhanced authority over their information.
2. Enforcing responsibility on Data Fiduciaries (entities determining the purpose and means of processing).
3. Promoting accountable creativity and developing confidence in India's electronic ecosystem.

Key Provisions of the DPDP Rules, 2025

1. Phased Implementation

The Rules adopt a pragmatic, staggered timeline to allow organizations time to adapt:

Immediate effect (November 13, 2025): Rules 1, 2, and 17–21 (short title, definitions, governance, and DPB-related provisions).[4]

After 12 months: Rule 4 (Consent Managers).

After 18 months (around May 2027): Core obligations under Rules 3, 5–16, 22, and 23 (notices, security, breaches, rights exercise, etc.).

1. Gradual Execution
   1.1. the Rules and Regulations follow a practical phased schedule to give entities duration to adjust :
   1.2. Instant enforcement (November 13, 2025): Rules 1,2, and 17 -21 (short title, definitions, governance, and DPB- related provisions)
   1.3. After 12 months: Rule 4 (consent Managers)
   1.4. After 18 months (around May 2027) : Core obligations under Rules 3, 5 -16, 22 and 23 (notices, security, breaches, rights exercise, etc,)
2. Notices and approval
   Data Fiduciaries must furnish a separate, lucid, and simple worded notification to Data Principles before handling. It has to contain an detailed explanation of individual information, defined objectives, and simple methods for revocation of approval, utilizing entitlements, or submitting grievances. Approval has to be voluntary, precise, knowledgeable, unrestricted, and clear.

3. Approval Administrators
   Enrolled organizations (fulfilling financial threshold), management, and autonomy standards) shall function as compatible systems for handling approval. They are required to enrol with the DPB and comply to rigorous duties for openness and safety.

4. Security Safeguards and Breach
   Notification Data Fiduciaries are required to apply appropriate safety measures, such a encoding, entry restrictions, recording, copies, and agreement based duties with Data

[4] Digital Personal Data Protection Rules, 2025, Rule 1(2)–(4), G.S.R. 846(E) (Nov. 13, 2025).

Processors. Logs and data must be retained for at least one year for adherence and inquiry objectives. On a violation, impacted persons have to be informed quickly with particulars of the violation, results, reduction steps, and communication details. The DPB has tobe notifies without postponement, with a comprehensive statement before 72 hours (or extended of allowed).

5. Data Retention and Erasure
   Personal data has to be deleted when the defined objectives is fulfilled, subject to a lowest one year preservation for records and linked information (except extended preservation is lawfully mandated). Particular preservation durations pertain to specific categories of Data Fiduciaries as according to timetable.

6. Special Protections Children
   Verifiable parental Consent is compulsory, with impairments; confirmable approval from legal protectors, confirmed under applicable legislations (e.g. Entitlements of Persons with Disabilities Act, 2026).

7. Significant Data Fiduciaries (SDFs)
   Some organizations (depending on quantity, delicacy, or effect) encounter increased duties, such as external reviews, Data Protections Impact Assessment (DPIAs), designation of a Data Protection Officer (DPO0, and formula based evaluations.

8. Data Protection Board of India
   Is a online priority rntity with up to four officials. It manages grievances, investigations, and execution through an internet based gateway and application. Challenges go to the Telecommunication Dispute Settlement and Appellate Court (TDSAT)

9. Processing for State Purposes
   Particular benchmarks pertain to state handling for aids, advantages, and facilities, stressing legal and safe management .

Implications for Stakeholders

For individuals, the Rules reinforce entitlements to retrieval, rectification, deletion, designation, and complaint resolution (with replies required before 90 days) for enterprises, particularly SDFs and entities managing extensive information, adherence demands substantial expenditure in procedures, systems, and management, however provides a definite route to develop customer confidence. Fines under the parent act continue substantial up to 250 rupees crore for safety and 200 crore rupees for violation disclosure or minor information infringements.[5]

Challenges and Way Forward

Although the regulations offer essential clearness, execution difficulties encompass creating strong Consent Manager ecosystems, guaranteeing confirmable approval systems, and aligning

[5] Digital Personal Data Protection Act, 2023, Schedule (Penalties), § 33.

with current legislations.[6] The gradual schedule provides relaxation space, however entities ought to start deficiency evaluation and action plan preparation right away. The structure establishes India as a accountable electronic country, balancing confidentiality with financial development. Continuous direction from MeitY and he DPD shall be vital for seamless implementation.[7]

Although the Rules provide essential clearness, execution difficulties encompass developing strong Consent Manager ecosystems, guaranteeing confirmable approval procedures, and aligning with current legislations. The gradual schedule provides relaxation space, however entities ought to start deficiency evaluations and strategy preparation right away.

The structure establishes India as a accountable electronic country, balancing confidentiality with financial development. Continuous direction from MeitY and the DPB shall be vital for seamless deployment.

Conclusion

The DPDP Rules, 2025, convert the 2023 Act from theory to application. By highlighting openness, responsibility and individual enablement, they establish the base for a reliable electronic environment in India. As implementation stages in, anticipatory adherence shall be essential to utilizing the prospects of the electronic era while protecting basic entitlements.

The DPDP Rules, 2025, transform the 2023 Act from principle to practice. By emphasizing transparency, accountability, and user empowerment, they lay the foundation for a trusted digital ecosystem in India. As enforcement phases in, proactive compliance will be key to harnessing the opportunities of the digital age while safeguarding fundamental rights.

References

1. Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (Nov. 13, 2025) (India), available at https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf.
2. The Digital Personal Data Protection Act, 2023, No. 22 of 2023 (Aug. 11, 2023) (India).
3. Press Information Bureau, Ministry of Electronics and Information Technology, DPDP Rules, 2025 Notified (Nov. 17, 2025).
4. PwC India, MeitY Notifies Digital Personal Data Protection Rules, 2025 (Nov. 16, 2025).

[6] Press Information Bureau, MeitY Notifies DPDP Rules, 2025 (Nov. 17, 2025).
[7] PwC India, Regulatory Insights: MeitY Notifies DPDP Rules, 2025 (Nov. 16, 2025).