[recovered from the vector store — dpdp_implementation_timeline_2025.txt p.1]

DIGITAL PERSONAL DATA PROTECTION RULES 2025 — OFFICIAL IMPLEMENTATION TIMELINE

Source: Gazette of India, G.S.R. 846(E), dated 13 November 2025 (MeitY notification)

==========
SECTION 1: STATUS OF THE RULES
==========

The DPDP Rules, 2025 were officially notified by the Ministry of Electronics and Information Technology (MeitY) on 13 November 2025 via Gazette notification G.S.R. 846(E).

These are FINAL NOTIFIED RULES — not a draft, not a public consultation document.
The January 2025 version was the draft circulated for consultation; the November 2025 Gazette notification is the official, enforceable version.

The Rules supersede and replace all earlier draft versions.

==========
SECTION 2: PHASED IMPLEMENTATION SCHEDULE
==========

The DPDP Rules, 2025 come into force in three phases:
PHASE 1 — 13 NOVEMBER 2025 (ALREADY IN FORCE)
Rules that came into force immediately on notification date:
- Rule 1: Short title and commencement
- Rule 2: Definitions (interpretation provisions)
- Rules 17–21: Data Protection Board of India (DPBI) constitution, procedure, and jurisdiction; bar of civil court jurisdiction

These rules are purely administrative. No substantive data processing obligations arise from Phase 1.

PHASE 2 — 14 NOVEMBER 2026
Rule coming into force:
- Rule 4: Consent Manager — registration, eligibility, obligations, and operational framework for entities seeking to act as Consent Managers under Section 6 of the DPDP Act, 2023.

PHASE 3 — 14 MAY 2027 (FULL SUBSTANTIVE OBLIGATIONS)
Rules coming into force — ALL remaining substantive provisions:
- Rule 3: Notice requirements (content, language, manner of notice to Data Principals)
- Rules 5–16: Consent management, children's data and parental consent, processing by schools, security safeguards, data retention, breach notification (72-hour rule), data principal rights (access, correction, erasure, nomination), duties of Data Fiduciaries, Significant Data Fiduciary obligations, Data Protection Officer appointment
- Rule 22: Cross-border data transfer restrictions and permitted jurisdictions
- Rule 23: Penalties — monetary penalties for violations become enforceable from 14 May 2027

KEY IMPLICATION: No substantive compliance obligations (notice, consent, parental consent, data security, breach reporting, erasure, penalties) are enforceable against any entity until 14 May 2027. Phase 3 is the effective compliance deadline for all organisations.

==========
SECTION 3: WHAT THIS MEANS FOR SPECIFIC SECTORS
==========
SCHOOLS AND EDUCATIONAL INSTITUTIONS:
- Rules governing processing of children's data and verifiable parental consent (Rules 9-10) do not apply until 14 May 2027.
- Schools have approximately 18 months from the Rules notification (Nov 2025 to May 2027) to prepare for full compliance.
- Preparatory steps for schools in this window:
  1. Audit all data flows: admissions, student records, CCTV, EdTech platforms, staff data
  2. Review third-party vendor agreements (ERP, exam platforms) — schools are Data Fiduciaries and liable for their Data Processors
  3. Draft compliant privacy notices in plain language (requirement under Rule 3)
  4. Design verifiable parental consent mechanism (not a checkbox — must be demonstrable)

5. Appoint a Grievance Officer; if the school qualifies as Significant Data Fiduciary, appoint a Data Protection Officer
6. Set data retention and erasure timelines for data of students who have left

GENERAL COMPLIANCE TIMELINE FOR ALL DATA FIDUCIARIES:
- Immediate (Phase 1 in force): No data processing obligations — Board being constituted
- By 14 Nov 2026: If operating as a Consent Manager, register under Rule 4
- By 14 May 2027: Full compliance with notice, consent, security, rights, breach reporting and cross-border transfer rules required

==========
SECTION 4: KEY PROVISIONS SUMMARY (PHASE 3 — EFFECTIVE MAY 2027)
==========

NOTICE (Rule 3 / Section 5):
- Data Fiduciary must provide notice before or at time of collecting personal data
- Notice must state: purposes of processing, goods/services to be provided, how to withdraw consent, how to exercise rights, how to file complaint with DPBI
- Notice must be in simple, plain language; accessible in multiple languages as notified

CONSENT (Rule 4 referred, Section 6):
- Consent must be free, specific, informed, unconditional, and unambiguous (affirmative action)
- Consent request must be presented separately from other terms
- Right to withdraw consent at any time; withdrawal must be as easy as giving consent
- Data must be erased within reasonable time after consent withdrawal (unless another lawful basis applies)

CHILDREN'S DATA (Rules 9–10 / Section 9):
- "Child" defined as a person below 18 years
- Verifiable parental consent required before processing child's personal data
- Data Fiduciaries must not process data in a manner detrimental to children's wellbeing
- Tracking, behavioural monitoring, and targeted advertising to children prohibited
- Schools and educational institutions may have limited carve-outs for educational purposes subject to Central Government notifications (exact scope to be notified before May 2027)

SECURITY SAFEGUARDS (Rule 8 / Section 8(5)):
- Reasonable security safeguards to prevent personal data breach
- Breach notification to DPBI and affected Data Principals within 72 hours of becoming aware

DATA PRINCIPAL RIGHTS (Rules 12–15 / Sections 11–14):
- Right to access: summary of personal data processed, identities of Data Fiduciaries shared with
- Right to correction and erasure
- Right of grievance redressal
- Right to nominate a nominee for exercise of rights after death/incapacity

SIGNIFICANT DATA FIDUCIARIES (Rule 16 / Section 10):
- Govt notifies entities as SDF based on: volume/sensitivity of data, national security risk, public order risk, rights of children, sovereignty risk
- SDFs must: appoint DPO (India-based), appoint independent Data Auditor, conduct periodic DPIA, carry out audits, comply with additional obligations as notified

PENALTIES (Rule 23 / Section 33):
- DPBI may impose financial penalties after inquiry
- Maximum penalty: up to Rs. 250 crore (for breach of children's data obligations)
- Other penalties: Rs. 50 crore to Rs. 200 crore depending on the nature of violation
- Penalties enforceable from 14 May 2027 (Phase 3)

CROSS-BORDER TRANSFERS (Rule 22 / Section 16):
- Transfer of personal data outside India permitted only to countries/territories notified by Central Government (whitelist approach)
- Notified countries list not yet published as of November 2025 — to be published before May 2027

==========
SECTION 5: REGULATORY STRUCTURE
==========

DATA PROTECTION BOARD OF INDIA (DPBI):
- Constituted under Chapter VI (Sections 18–27) of DPDP Act, 2023

- Rules 17–21 governing DPBI constitution are in force since Phase 1 (13 Nov 2025)
- DPBI adjudicates: complaints from Data Principals, references from Central Government, suo motu action for significant breaches
- DPBI decisions are appealable to High Court
- Civil courts have no jurisdiction over matters under the DPDP Act (Section 55)

CENTRAL GOVERNMENT ROLE:
- Notifies Significant Data Fiduciaries (Section 10)
- Notifies permitted countries for cross-border transfers (Section 16)
- May exempt categories of Data Fiduciaries from certain obligations (Section 17)
- May issue directions to DPBI (Section 36)

==========

END OF DOCUMENT

==========