pricoris
Building Trustworthy Digital Ecosystem

Mastering the DPDP Act 2023 & DPDP Rules 2025 — A Practical Handbook for Compliance, Implementation and Training

Mastering the DPDP Act 2023 & DPDP Rules 2025

A Practical Handbook for Compliance, Implementation and Training

(Pricoris LLP — 2025 Edition)

Contents

Executive Summary

India's transition to a digital economy has brought millions of individuals, businesses and public systems online. With this shift, personal data is generated at a scale never seen before — through apps, transactions, healthcare systems, travel platforms, HR systems, logistics, and everyday customer interactions.

The **Digital Personal Data Protection Act, 2023** and the **DPDP Rules, 2025** together create a modern, enforceable privacy framework that every organisation must now operationalise.

The intent is clear:

- Empower individuals
- Hold organisations accountable
- Create predictable privacy governance
- Build trust in India's digital ecosystem

This whitepaper explains the DPDP law in a **clear and operational** manner — without legal jargon. It focuses on:

- rewriting notices and consent journeys
- implementing Section 7 legitimate-use registers
- rights-handling SOPs and audit trails
- retention & erasure logic
- breach governance
- children & PWD processing
- SDF obligations
- processor contracting requirements
- training modules for DPOs, HR, IT, Security, Legal, CX & Product teams

The objective is simple: **help organisations embed DPDP compliance into daily workflows**, instead of treating it as a documentation exercise.

1. Understanding the DPDP Architecture

DPDP is built as a 3-layer framework. Each layer plays a distinct role in compliance.

A. The Act (Chapters 1–9)

The Act provides the foundation. Key elements include:

- definitions (Data Principal, Data Fiduciary, Data Processor, SDF, child, etc.)
- applicability rules
- lawful grounds (consent + legitimate use)
- duties of DFs & DPs
- rights of individuals
- breach and grievance requirements
- DPB's structure, powers, penalties & appeals

The Act sets the "**what**".

B. The Rules (23 Rules)

The Rules operationalise the Act. They define the "how".

Key operational areas:

- Rule 3 – notice requirements
- Rule 4 – consent manager (for entities choosing to use them)
- Rule 5 – special-purpose processing
- Rule 6 – security safeguards
- Rule 7 – breach notification
- Rule 8 – retention, erasure & inactivity rules

• Rule 9 – DPO/representative contact details
• Rule 10–12 – children & PWD processing
• Rule 13 – SDF obligations

Rule 14- Rights of Data Principals
• Rule 15 – cross-border transfer conditions

Rule 16 — Exemptions for Research, Archiving, and Statistical Purposes

Rule 17-23 – Rules for Data Protection Board

C. The Seven Schedules

A major improvement in accuracy over older drafts — these seven schedules matter operationally:

1. **Schedule I — Consent Manager Requirements**
2. **Schedule II — Security Safeguards for notified Government entities**
3. **Schedule III — Three-year Inactivity Rule + 48-hour Pre-Erasure Notice**
   (For large e-commerce, gaming, social media platforms)
4. **Schedule IV — Exceptions for Children & PWD Data (real-time safety, emergency use)**
5. **Schedule V & VI — Terms and conditions of service of Bosrd members**
6. **Schedule VII — Mandatory 1-Year Retention for Certain Sovereign/Statutory Functions**

Together, these elements form India's complete privacy regime.

2. Obligations of Data Fiduciaries — What Teams Must Actually Do

Most organisations want a clear, operational checklist. DPDP requires organisations to:

A. Draft DPDP-compliant Notices (Rule 3)

• itemised list of personal data
• purpose-specific (no bundled purposes)
• rights + grievance
• languages (English or Eighth Schedule)
• accessibility

• change notifications
• withdrawal mechanism

B. Redesign Consent Journeys

Consent must be:

- Free
- Specific
- informed
- unambiguous
- unconditional
- based on affirmative action

"Equal ease" withdrawal is mandatory. Pre-ticked boxes and continued-use consent banners are invalid.

C. Maintain a Section-7 Legitimate Use Register

For each legitimate-use case:
• purpose
• voluntary provision
• absence of refusal
• data minimisation logic
• audit trail

This is critical for GDPR-compliant companies adjusting to DPDP.

D. Establish Rights-Handling Workflows

Rights include:
• access
• correction
• completion
• updating
• erasure
• grievance
• nomination

DFs have 90 days to respond. Identity verification and registers are mandatory.

E. Implement Breach Governance

• immediate notice to Data Principals
• immediate notice to DPB
• detailed second report within 72 hours
• breach register
• remediation records

F. Apply Retention & Erasure Logic (Section 8(7) + Rule 6)

- erase data once purpose is complete
- erase upon withdrawal of consent
- maintain logs for 1 year
- apply Third Schedule rules for large platforms

Retention must be mapped category-wise.

G. Contract Management

Vendor contracts must include:
- security safeguards
- cooperation in breach notifications
- retention & erasure obligations
- restrictions on sub-processing
- DPDP-specific log retention clauses

H. Operational Governance & Dashboards

Leadership needs visibility across:
- notices
- consent flows
- DSAR volumes
- breach incidents
- data retention metrics
- vendor readiness
- SDF impact

DPDP expects *measurable governance*.

3. Training Framework for Organisations

Your training programme is a key differentiator. It makes compliance practical.

Module 1 — The DPDP Act Explained

Principles, roles, applicability, enforcement design.

Module 2 — Notice & Consent Workshop

Rewrite real notices; fix UX; apply itemisation; build withdrawal journeys.

Module 3 — DSAR Bootcamp

- verification flows
- refusal grounds
- evidence trails

• response templates
• registers & SLA systems

Module 4 — Breach Response Tabletop

Draft notices to DP + DPB; run simulations.

Module 5 — Retention & Erasure

Real case studies:
• Third Schedule
• Schedule VI logs
• Purpose-completion rules

Module 6 — Children & PWD Data

Risk-based scenarios; guardian verification; prohibited tracking.

Module 7 — Significant Data Fiduciary Track

• DPIA
• independent audits
• algorithmic due diligence
• Board reporting

Module 8 — Vendor Oversight

Sub-processing, retention flow-downs, contract clauses.

4. A Practical Compliance Roadmap (12–18 Months)

A timeline organisations can adopt immediately.

Months 1–2: Foundations

• data inventory & mapping
• confirm DF/DP roles
• scope systems & flows

Months 3–4: Notices & Consent

• rewrite all privacy notices
• validate consent patterns
• create Section-7 Register

Months 5–6: Rights & Grievance

- DSAR portal
- identity verification
- escalation matrix

Months 7–9: Breach & Vendor Governance

- breach tabletop
- incident logging
- vendor contract updates
- security safeguards roll-out

Months 10–12: Risk & Governance

- DPIAs
- governance dashboards
- policies & procedures

Months 13–18: Maturity

- internal audits
- training refresh
- automation
- ongoing monitoring & review

5. Templates Included (DPDP Toolkit)

Your downloadable toolkit will include:

✓ privacy notice
✓ consent SOP
✓ DSAR register
✓ breach register
✓ data protection agreement
✓ legitimate-use register
✓ retention table
✓ children's data SOP
✓ PWD verification SOP
✓ exemptions cheat sheet
✓ SDF readiness checklist

6. Conclusion — Why DPDP Requires Structured, Ongoing Governance

DPDP marks a structural change in how Indian organisations handle personal data. Compliance is not a one-off exercise. Organisations must **show evidence of accountability**, redesign processes, and build privacy into daily operations.

A mature compliance programme integrates:
• GDPR foundations
• ISO 27701 governance alignment
• India-specific legal requirements under DPDP
• operational evidence through registers, dashboards & workflows

Training, templates, and structured governance together create a compliance posture that is defensible, auditable, and ready for enforcement.

Pricoris LLP's DPDP framework is designed to help organisations reach this level efficiently and with confidence.