MYITMANAGER.IN

Cybersecurity & Data Protection Consulting | myitmanager.in

Edition: April 2026 | DPDP Rules 2025 Final

DPDP Act Compliance Checklist 2026

Digital Personal Data Protection Act, 2023 + DPDP Rules 2025

8	65+	RAG	■250Cr
Compliance Categories	Action Items	Maturity Scoring	Max Penalty

What's inside:

- ✓ Consent & Notice obligations
- ✓ Data Principal rights framework
- ✓ Security safeguards checklist
- ✓ Breach notification requirements
- ✓ Sector tags: SaaS · Fintech · Healthtech · E-commerce
- ✓ Penalty reference table & enforcement timeline

DPDP Enforcement Timeline

Now	Nov 2026	May 2027
Phase 1 begins Core obligations active	Consent Manager registration deadline	Full enforcement All provisions operational

How to Use This Checklist

Step 1	**Work through each section.** Tick every item your organisation currently meets. Leave unticked items blank — they are your gaps.
Step 2	**Score each section.** Count your ticks and enter in the Score Box at the end of each section. Less than 50% = RED, 50–99% = AMBER, all ticked = GREEN.
Step 3	**Use the Compliance Tracker** (last page) to assign an Owner and Target Date to every section showing RED or AMBER.
Step 4	**Sector tags** (SaaS, Fintech, Health, E-com) highlight items with heightened obligations for your industry. Treat these as priority items.

■ **GREEN — Compliant**	All items in section checked. Maintain and evidence.	■ **AMBER — Partial**	50–99% complete. Prioritise remaining gaps.	■ **RED — High Risk**	Under 50% complete. Immediate remediation needed.

Sector Tags

SaaS — heightened obligation for cloud-hosted personal data	**Fintech** — additional RBI / SEBI intersection	**Health** — health data = sensitive personal data under DPDP	**E-com** — consumer-facing data volume + payment data

✓ 1. Lawful Basis & Consent Management

- ☐ Identify all personal data processing activities and map to a lawful basis (consent or legitimate use)
- ☐ Consent requests written in plain, simple language — no legalese, no bundled consent
- ☐ Consent is freely given, not conditioned on a service the individual is entitled to receive
- ☐ Consent Notice includes: identity of Data Fiduciary, purpose, Data Principal rights, how to withdraw
- ☐ Withdrawal mechanism is as easy as giving consent — tested and functional SaaS
- ☐ Consent records maintained: timestamp, version of notice, channel, and IP SaaS
- ☐ Consent re-obtained whenever purpose of processing changes
- ☐ Employee HR data has separate consent flows distinct from customer data
- ☐ Consent Manager appointed or registered (if acting as Consent Manager platform) All

Section 1 Score ___ / 9 ■ All checked = GREEN ■ 50–99% = AMBER ■ <50% = RED

2. Notice & Transparency

- ☐ Privacy Notice covers: data collected, why, retention period, who it is shared with
- ☐ Notice available in English and at least one Eighth Schedule language
- ☐ Notice provided before or at the time of collection — not buried in Terms & Conditions
- ☐ Notice accessible without requiring login or account creation SaaS
- ☐ Data collection forms indicate which fields are mandatory vs optional E-com
- ☐ Notice updated and republished whenever processing purposes change
- ☐ All versions of Privacy Notice archived with effective dates
- ☐ Website/app has a clearly labelled and accessible Privacy Policy link E-com

Section 2 Score ___ / 8 ■ All checked = GREEN ■ 50–99% = AMBER ■ <50% = RED

■ 3. Data Principal Rights

- ☐ Process in place to receive and fulfil Right to Access requests within defined SLA
- ☐ Data Principal can request a summary of personal data held and all processing purposes
- ☐ Right to Correction: mechanism to update inaccurate or incomplete personal data
- ☐ Right to Erasure: deletion request triggers removal across all systems including backups (within retention policy) SaaS
- ☐ Right to Grievance Redressal: DPO/contact point published and responsive within 30 days
- ☐ Right of Nomination: mechanism for individual to nominate another in case of death or incapacity
- ☐ All rights requests logged: date received, action taken, date resolved
- ☐ Rights fulfilment workflow tested at least once per year
- ☐ Automated rights request intake (web form or email alias) — not manual only SaaS

Section 3 Score ___ / 9 ■ All checked = GREEN ■ 50–99% = AMBER ■ <50% = RED

■ 4. Data Fiduciary Obligations

- ☐ Data Protection Officer (DPO) appointed if classified as Significant Data Fiduciary (SDF)
- ☐ DPO is based in India and reports directly to the Board (not just management)
- ☐ Independent Data Auditor appointed for SDF — annual audit conducted and report filed
- ☐ Data Protection Impact Assessment (DPIA) conducted for all high-risk processing activities
- ☐ Data minimisation enforced — only data necessary for the stated purpose is collected SaaS
- ☐ Purpose limitation enforced — data not used beyond consented purpose without fresh consent
- ☐ Storage limitation policy: data deleted or anonymised when purpose is fulfilled Health
- ☐ Data accuracy controls ensure personal data is correct and up to date
- ☐ Register of all processing activities maintained and reviewed quarterly

Section 4 Score ___ / 9 ■ All checked = GREEN ■ 50–99% = AMBER ■ <50% = RED

■ 5. Security Safeguards (Section 8)

- ☐ Encryption of personal data at rest and in transit (TLS 1.2+, AES-256 or equivalent) Fintech
- ☐ Role-based access controls (RBAC) — personal data accessible on need-to-know basis only
- ☐ Access logs maintained across all personal data systems — retained for minimum 12 months SaaS
- ☐ Vulnerability Assessment & Penetration Testing (VAPT) conducted at least annually by qualified firm
- ☐ Patch management: critical vulnerabilities remediated within 30 days of disclosure
- ☐ Multi-factor authentication (MFA) enforced for all systems processing personal data Fintech
- ☐ Data Loss Prevention (DLP) controls in place for sensitive personal data categories Health
- ☐ Third-party security assessment for every vendor with access to personal data
- ☐ Security awareness training for all employees — at least annually, with attendance records
- ☐ Incident response plan documented, tested, includes DPDP breach notification workflow

Section 5 Score ___ / 10 ■ All checked = GREEN ■ 50–99% = AMBER ■ <50% = RED

6. Data Breach Notification

- [ ] Breach detection mechanisms: SIEM, alerting, monitoring across all personal data systems Fintech
- [ ] Breach classification process: defines what constitutes a "reportable" breach under DPDP
- [ ] Process to notify Data Protection Board of India (DPBI) promptly upon discovery
- [ ] Process to notify affected Data Principals with clear, plain-language communication
- [ ] Breach notification template prepared and approved in advance — not drafted during an incident
- [ ] Breach register maintained — all incidents logged regardless of reportability threshold
- [ ] Post-breach root cause analysis and remediation actions documented and reviewed
- [ ] Breach response tabletop exercise conducted at least annually SaaS

Section 6 Score ___ / 8 ■ All checked = GREEN ■ 50–99% = AMBER ■ <50% = RED

■ 7. Data Processors & Third Parties

- ☐ Inventory of all Data Processors (vendors processing personal data on your behalf)
- ☐ Data Processing Agreement (DPA) signed with every Data Processor before data sharing
- ☐ DPA binds processor to process data only per Data Fiduciary instructions
- ☐ Data Processors prohibited from engaging sub-processors without prior written approval SaaS
- ☐ Annual security assessment or audit of all critical Data Processors
- ☐ Cross-border data transfer only to countries notified by Central Government — verified Fintech
- ☐ Vendor contracts include data deletion/return obligations on exit or termination
- ☐ Processor breach notification clause: processor notifies Fiduciary immediately on discovery

Section 7 Score ___ / 8 ■ All checked = GREEN ■ 50–99% = AMBER ■ <50% = RED

8. Children's Data & Special Obligations

- ☐ Age verification mechanism identifies users under 18 before processing their data — E-com
- ☐ Verifiable parental consent obtained before processing personal data of children
- ☐ Processing detrimental to children's well-being prohibited — controls implemented and tested
- ☐ Behavioural tracking, targeted advertising, and profiling of children strictly prohibited — E-com
- ☐ Privacy-by-design applied to product features accessible by children — SaaS
- ☐ Children's data not shared with third parties without explicit parental consent
- ☐ Age gate implemented if platform is not intended for users under 18 — E-com

Section 8 Score ___ / 7 ■ All checked = GREEN ■ 50–99% = AMBER ■ <50% = RED

Penalty Reference — DPDP Act 2023 Schedule

Penalties are cumulative per breach and may be imposed by the Data Protection Board of India (DPBI).

Violation	Max Penalty	Risk	Primary Section
Failure to implement reasonable security safeguards	■ 250 Crore	CRITICAL	Section 5 — Security
Failure to notify data breach to DPBI or Data Principal	■ 200 Crore	CRITICAL	Section 6 — Breach
Non-compliance with children's data processing obligations	■ 200 Crore	CRITICAL	Section 8 — Children
Failure to fulfil Data Principal rights (erasure, correction, nomination)	■ 50 Crore	HIGH	Section 3 — Rights
Failure to register as Consent Manager (if applicable)	■ 50 Crore	HIGH	Section 1 — Consent
Breach of any other provision of the Act	■ 50 Crore	MEDIUM	All sections

Compliance Tracker

#	Section	RAG	Score (__/__)	Owner	Target Date	Notes / Next Action
1	Consent Management		__ / 9			
2	Notice & Transparency		__ / 8			
3	Data Principal Rights		__ / 9			
4	Data Fiduciary Obligations		__ / 9			
5	Security Safeguards		__ / 10			
6	Breach Notification		__ / 8			
7	Data Processors		__ / 8			
8	Children's Data		__ / 7			

OVERALL SCORE: _____ / 68 items

0–34 = RED (High Risk) 35–61 = AMBER (Partial) 62–68 = GREEN (Compliant)

Ready to implement? We can help.

MYITMANAGER.IN delivers end-to-end DPDP Act compliance — from gap assessment to board-ready reporting. Trusted by 100+ Indian organisations including Zomato, Tata 1mg, Magicpin, RenewBuy, and EnableX.

Gap Assessment & Roadmap	**Consent Framework Design**	**DPO Advisory & Support**	**Breach Response Planning**	**ISO 27001 & SOC 2 Combined**

■ **https://myitmanager.in**

✉■ **help@myitmanager.in**

■ India (Pan-India & Remote)