The **Digital Personal Data Protection Act, 2023** is India's first comprehensive data-protection law, and with the final **DPDP Rules, 2025** notified, every Indian SME with a website, a payroll system, or a customer list is on a countdown to **14 May 2027** — the day the substantive obligations become enforceable. This guide compresses what a 50-to-200-person SME must do into one working document: the timeline, the obligations, a five-phase rollout, and the seven mistakes that cost SMEs most. Full guide: vcisodesk.com/dpdp-act-compliance-guide-indian-smes/.

The dates and numbers that anchor everything

Law + Rules: DPDP Act assented 11 Aug 2023; final DPDP Rules, 2025 notified via Gazette G.S.R. 846(E) (dated 13 Nov 2025, published 14 Nov 2025).

Phase I — in force since 14 Nov 2025: definitions, Data Protection Board framework, adjudication procedure (Rules 1, 2, 17–21). Caveat: the Board is constituted in law but **not yet operational** — no members appointed as of mid-2026.

Phase II — 14 Nov 2026: Consent Manager framework (Rule 4) — registration, eligibility, conduct standards. Pick your counterparty during this window if you won't build consent infrastructure in-house.

Phase III — 14 May 2027: all substantive fiduciary obligations crystallise — notice & consent, data principal rights, breach notification, retention limits, processor contracts, security safeguards.

Penalty ceilings (Schedule): ₹250 crore — failure of reasonable security safeguards · ₹200 crore — failure to notify breaches · ₹200 crore — children's-data failures · ₹150 crore — SDF obligation failures.

Plan for sooner: in Jan 2026 MeitY floated compressing the 18-month window to 12 months. Not law yet — but build for 'sooner', not 'later'.

1. Know your role (the Act renames what you already do)

Role	Who it is in your SME
Data fiduciary	You — whenever you decide why and how personal data is processed: customer records, payroll, marketing lists.
Data processor	Your vendors processing data on your behalf: CRM, payroll service, cloud email, hosting. You remain accountable for them.
Data principal	The individual the data is about — customer, employee, candidate. For children (under 18, s.2(f)), the parent/lawful guardian consents; verifiable parental consent is not required for certain essential services (healthcare, education, child safety).
Significant Data Fiduciary	A category the Centre can notify (s.10) by volume/sensitivity — triggers a resident DPO, independent audits, and DPIAs. Most SMEs are not SDFs; no numeric thresholds notified as of mid-2026 — watch for the notification.

2. Rights your customers and employees can now exercise against you

R1 Access — what personal data you process, the processing activities, and who it has been shared with. ☐

R2 Correction & erasure — fix inaccurate data; erase when no longer necessary or when consent is withdrawn. ☐

R3 Grievance redressal — they complain to you first; you must publish a response timeline **not exceeding 90 days** (Rule 14(3)) and meet it. Only then can they escalate to the Board. ☐

R4 Nomination — another individual may exercise rights on death or incapacity. ☐

R5 Withdraw consent — as easily as it was given; triggers forward-looking erasure obligations. ☐

Operational implication: a published channel (an email address is fine, a form is better) plus a monitored internal process. A privacy@ inbox nobody reads is worse than no inbox.

3. Core fiduciary obligations — the compliance checklist

O1 Notice & consent at or before collection — categories collected, purposes, how to exercise rights, how to complain to the Board. Consent must be free, specific, informed, unconditional, unambiguous — no pre-ticked boxes, no bundled consents. ☐

- [ ] **O2 Privacy notice** published in plain language — what you collect, why, retention, sharing, and rights channels.
- [ ] **O3 Purpose-specific opt-ins** for anything beyond the transaction — marketing, analytics, profiling each need their own clear consent.
- [ ] **O4 Data Processing Agreements** with every processor — DPDP-equivalent obligations, purpose restriction, assistance with requests, prompt breach notification. Read the DPA; do not assume standard terms cover it.
- [ ] **O5 Breach notification (Rule 7, two-stage)** — intimate each affected data principal AND the Board "without delay"; detailed report to the Board **within 72 hours** (extendable only on written request). Detection-to-notification must be measured in hours.
- [ ] **O6 Reasonable security safeguards** — encryption, access control, logging, secure deletion, documented incident response. Highest penalty tier (₹250 cr) attaches here. The Rules add a concrete floor: logs and breach-relevant data retained **at least one year**.
- [ ] **O7 Retention discipline** — documented retention period per data category; erase when the purpose is done unless another law (tax, employment, KYC) requires retention.
- [ ] **O8 Record-keeping** — data inventory, purposes, data-principal categories, retention schedule, processor list, consent records — producible on request.
- [ ] **O9 Named contact** for data-principal requests (a statutory DPO is only required for SDFs).

4. Five-phase rollout for a 50–200 person SME

- [ ] **P1 Month 1 — Audit.** Map every system holding personal data: what data, whose, purpose, retention, access, consent status. This data inventory is the foundation document.
- [ ] **P2 Month 2 — Notices & consent.** Rewrite the privacy notice; upgrade consent capture on every form; decide lawful basis (consent vs legitimate uses) per processing category; plan a fresh-notice campaign for historical data.
- [ ] **P3 Month 3 — Technical measures.** Encryption in transit/at rest, role-based access, logging, secure deletion, incident response plan. Overlaps CERT-In baseline controls — run as one workstream.
- [ ] **P4 Months 4–6 — Processes & staff.** Data-principal-request workflow, DPAs with every processor, staff training, breach runbook with Board + data-principal templates.
- [ ] **P5 Ongoing.** Quarterly access reviews, annual notice refresh, retention runs, yearly internal audit, watch for SDF notification criteria.

5. The seven mistakes that cost SMEs most

- [ ] **M1** Vague or bundled consent — "by clicking Sign Up you agree to everything" is not DPDP-grade consent.
- [ ] **M2** The 2019 copy-pasted privacy notice — rewrite for your actual categories and purposes.
- [ ] **M3** Over-retention — "just in case" data is now penalty exposure, not an asset.
- [ ] **M4** Vendors without DPAs — quickest wins: CRM, payroll, email platform, analytics.
- [ ] **M5** No staff training — a 45-minute onboarding session plus annual refresh is the minimum defensible baseline.
- [ ] **M6** No breach response plan — pre-written templates and a named "is this reportable?" decision-maker are non-negotiable; the clock is measured in hours.
- [ ] **M7** Ignored data-principal requests — every unlogged request is a future complaint to the Board.

6. DPDP alongside CERT-In and ISO 27001

The three frameworks answer different questions. **CERT-In** sets the technical security baseline and national incident-reporting duties. **DPDP** defines your obligations to the people whose data you hold. **ISO 27001** is the management-system scaffolding. The overlap (encryption, access control, logging, incident response) is real — run one programme, not three: start with CERT-In baseline controls, layer DPDP-specific obligations (consent, notices, rights, DPAs) on top, and consider ISO 27001 only when a customer or commercial requirement justifies it.

Content current as of 5 June 2026 — re-verify dates if MeitY notifies the proposed timeline compression. Full pillar guide: vcisodesk.com/dpdp-act-compliance-guide-indian-smes/ — free, like everything on GRC RADAR.