

## DATA PROTECTION REGIME, INDIA PHASE-WISE COMPLIANCE PLAYBOOK (Effective 13.11.2025)

(Based on GSR 843(E), 844(E), 845(E))

DPDP Act – Enforcement | DPB members | DPB establishment

### MASTER TIMELINE VIEW

Phase	Date	Compliance Areas
Phase 1	13 Nov 2025	Definitions, DPB establishment, rights redressal, breach readiness
Phase 2	13 Nov 2026	Consent Managers registration & operationalisation; Sec 27(1)(d) compliance
Phase 3	13 May 2027	Full compliance regime: notices, consent, breach, rights, children, SDF, DPIA, cross-border, exemptions

### PHASE WISE IMPLEMENTATION

<p><b>PHASE 1 — IMMEDIATE (Effective 13 November 2025)</b></p> <p><b>Sections in force:</b> Sec 1(2), 2, 18–26, 35, 38–44(1),(3)</p> <p><b>A. Legal &amp; Governance Setup</b></p> <ul style="list-style-type: none"> <li>▪ Review applicability of Act to business (Sec 2).</li> <li>▪ Identify entity role: Data Fiduciary / Data Processor.</li> <li>▪ Map all digital personal data inflows/outflows.</li> <li>▪ Update internal Grievance Redressal workflows (Sec 13).</li> <li>▪ Prepare for Data Principal rights: Access, Correction, Erasure, Nomination (Secs 11–14).</li> </ul> <p><b>B. Readiness for the DATA PROTECTION BOARD (DPB)</b></p> <ul style="list-style-type: none"> <li>▪ Note DPB established (GSR 844(E)).</li> <li>▪ Maintain breach-ready documentation (for DPB directions).</li> <li>▪ Align internal escalation matrix for DPB notices.</li> </ul> <p><b>C. Consent Manager &amp; Registration-Ready Framework</b></p> <ul style="list-style-type: none"> <li>▪ Prepare to integrate with DPB-registered Consent Managers (Sec 6(7),(10)).</li> <li>▪ Implement internal consent logs for later verification.</li> </ul>	<p><b>PHASE 2 — BY 13 NOVEMBER 2026 (1 YEAR DEADLINE)</b></p> <p><b>Sections coming into force:</b> Sec 6(9) + Sec 27(1)(d)</p> <p>DPDP Act - Enforcement</p> <p><b>A. Consent Manager Registration Compliance</b></p> <ul style="list-style-type: none"> <li>▪ Ensure all Consent Managers used by the entity are <b>DPB-registered</b>.</li> <li>▪ Update all consent flows to ensure <b>verifiable traceability</b>.</li> </ul> <p><b>B. Data Principal's RIGHT TO WITHDRAW VIA CONSENT MANAGER</b></p> <ul style="list-style-type: none"> <li>▪ Deploy seamless consent withdrawal workflow.</li> <li>▪ Automate “cease processing upon withdrawal” triggers.</li> </ul> <p><b>C. Blacklisting Obligations (Sec 27(1)(d))</b></p> <ul style="list-style-type: none"> <li>▪ (When DPB notifies blocking of a Data Fiduciary for repeated breaches.)</li> <li>▪ Set up system to detect/deny data sharing with “blocked” fiduciaries.</li> <li>▪ Build a vendor-risk list integrating DPB notifications.</li> </ul>
<p><b>PHASE 3 — BY 13 MAY 2027 (18 MONTH DEADLINE)</b></p> <p><b>Largest enforcement block:</b></p> <p>Secs 3–5, 6(1–8),(10), 7–10, 11–17, 27(except 1(d)), 28–34, 36–37, 44(2)</p> <p>DPDP Act - Enforcement</p> <p><b>A. FULL CONSENT, NOTICE &amp; LAWFUL PROCESSING OBLIGATIONS</b></p> <ul style="list-style-type: none"> <li>▪ Issue all notices under Sec 5 in English + 8th Schedule languages.</li> <li>▪ Verify “free, specific, informed, unconditional” consent (Sec 6).</li> <li>▪ Deploy consent-withdrawal parity (ease = ease of giving).</li> </ul> <p><b>B. SECURITY, BREACH &amp; DPIA FRAMEWORK (Core Compliance)</b></p> <ul style="list-style-type: none"> <li>▪ Implement robust technical + organisational security (Sec 8(4),(5)).</li> <li>▪ Deploy breach-notification SOP for DPB + affected Data Principals (Sec 8(6)).</li> <li>▪ Establish data-retention + erasure timelines (Sec 8(7),(8)).</li> <li>▪ Create a Data Lifecycle Register (collection, processing, deletion).</li> </ul> <p><b>C. CHILD DATA PROCESSING COMPLIANCE (Sec 9)</b></p> <ul style="list-style-type: none"> <li>▪ Implement parental verifiable consent.</li> <li>▪ Disable behavioural monitoring/tracking/ads for children.</li> <li>▪ Classify products/services impacting children.</li> </ul>	<p><b>PHASE 3.1 — BY 13 MAY 2027 (18 MONTH DEADLINE)</b></p> <p><b>D. SIGNIFICANT DATA FIDUCIARY (SDF) PREPAREDNESS (Sec 10) (<i>Only if notified by Govt later</i>)</b></p> <ul style="list-style-type: none"> <li>▪ Appoint a Data Protection Officer (India-based).</li> <li>▪ Appoint independent Data Auditor.</li> <li>▪ Conduct periodic DPIA.</li> <li>▪ Maintain audit trail of processing activities.</li> </ul> <p><b>E. DATA PRINCIPAL RIGHTS SYSTEM (Sec 11–14)</b></p> <ul style="list-style-type: none"> <li>▪ Create a unified rights-management portal to support:</li> <li>▪ Access</li> <li>▪ Correction/Erasure</li> <li>▪ Grievance resolution within prescribed timelines</li> <li>▪ Post-death nominee mechanism</li> </ul> <p><b>F. DATA TRANSFER RULES COMPLIANCE (Sec 16)</b></p> <ul style="list-style-type: none"> <li>▪ Verify if Central Government has <b>notified restricted geographies</b>.</li> <li>▪ Update cross-border contracts &amp; SCCs accordingly.</li> </ul> <p><b>G. EXEMPTIONS MANAGEMENT (Sec 17)</b></p> <ul style="list-style-type: none"> <li>▪ Identify lawful exemptions applicable to business lines.</li> <li>▪ Maintain logs for legal claims, law-enforcement exceptions.</li> </ul>

### DELIVERABLES

External	Internal
<p><b>External</b></p> <ul style="list-style-type: none"> <li>▪ Clean statutory timeline</li> <li>▪ Obligations summary</li> <li>▪ Industry-specific compliance roadmap</li> <li>▪ Breach response flowchart</li> <li>▪ Consent + Notice templates</li> </ul>	<p><b>Internal</b></p> <ul style="list-style-type: none"> <li>▪ Detailed Sec-wise compliance tracker</li> <li>▪ Clause bank for contracts (SaaS, DP agreements, processors)</li> <li>▪ DPIA templates</li> <li>▪ Grievance redressal timeline triggers</li> <li>▪ Enforcement impact tracker</li> <li>▪ SDF readiness checklist</li> </ul>