COMPLIANCE OPERATIONS · INDIA

DPDP Readiness Checklist

A practical, item-by-item control guide mapping notice workflows, consent-log requirements and Data-Principal rights-request processes to the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025.

PREPARED BY	VERSION	FRAMEWORK	CONTROLS
SilicaSecure Pvt. Ltd.	v1.0 · June 2026	DPDP Act 2023 + Rules 2025	64 items · 8 domains

How to use this checklist

Read first — scope, status workflow and priority legend.

What this is	An operational readiness checklist for any Data Fiduciary processing digital personal data of individuals in India. It turns the statutory duties into auditable, ownable line items. Work top-to-bottom by domain; assign each item an owner and capture evidence in the right-hand column.
Status workflow	Tick the Done box only when the control is live in production AND evidence exists (a document, link, log sample, or screenshot). 'Designed but not deployed' is not Done. Use the Owner column for the accountable person and the Evidence column to point at the proof.
Key deadlines	DPDP Rules, 2025 were notified on 13 November 2025. The Data Protection Board is already operational. Consent-Manager provisions take effect 13 November 2026. Full substantive compliance is due 13 May 2027 — there is no expected grace period. Penalties reach ₹250 crore for a security-safeguard failure and stack per contravention.

PRIORITY LEGEND

- **CRITICAL** Blocks lawful processing or creates direct penalty exposure — do first.
- **HIGH** Required for full compliance by 13 May 2027.
- **MEDIUM** Strengthens posture / situational (e.g. SDF-only).

Scope note: this checklist is a working tool, not legal advice. Verify every reference against the official Gazette text of the Act and Rules and any subsequent Data Protection Board guidance. Significant-Data-Fiduciary items apply only if your entity is notified as an SDF by the Central Government.

A Notice & transparency workflows

Itemised notices, withdrawal links, language access and legacy re-papering — Act s.5 / Rule 3.

ID	Checklist item / control	DPDP reference	Priority	Done	Owner	Evidence / notes
NT-01	Build a master inventory of every notice surface (web, app, checkout, forms, kiosks, IVR, partner pages) where personal data is collected.	Act s.5; Rule 3	CRITICAL	☐		*Map to data-flow register*
NT-02	Ensure each notice is itemised — lists the specific personal data sought and the specific purpose for each item, not a blanket statement.	Act s.5(1); Rule 3(a)	CRITICAL	☐		*No bundled purposes*
NT-03	Notice is written in clear, plain language and is available in English and the 22 Eighth-Schedule languages on request (Bhashini-ready).	Act s.5(3); Rule 3(b)	HIGH	☐		*Language toggle / API*
NT-04	Notice contains a working link/means to withdraw consent that is as easy to use as the means by which consent was given.	Act s.6(4)–(6); Rule 3	CRITICAL	☐		*Test the withdraw link*
NT-05	Notice contains the means to exercise Data Principal rights and to make a complaint to the Data Protection Board.	Act s.5(2); Rule 3(c)	CRITICAL	☐		*Link to rights portal + Board*
NT-06	Publish business/contact details of the DPO or designated person who answers data-processing questions.	Act s.8(9); Rule 9	HIGH	☐		*On notice + website footer*
NT-07	For consent obtained before the Act, issue a fresh compliant notice to legacy Data Principals 'as soon as reasonably practicable'.	Act s.5(2) proviso	HIGH	☐		*Legacy re-papering campaign*
NT-08	Version-control every notice; retain superseded versions with effective-from/-to dates as audit evidence.	Rule 6 (records)	MEDIUM	☐		*Immutable notice archive*
NT-09	Map each notice to its lawful basis (consent vs. legitimate use) and document why, before go-live.	Act s.4, s.7	HIGH	☐		*Basis register*
NT-10	QA workflow: legal sign-off gate so no new collection point ships without an approved, linked notice.	Internal control	MEDIUM	☐		*Add to release checklist*

Domain A — 10 controls. Mark Done only with evidence captured.

B Consent capture, log & withdrawal

Granular consent, append-only consent ledger, withdrawal handling — Act s.6 / Rule 6 / Second Schedule.

ID	Checklist item / control	DPDP reference	Priority	Done	Owner	Evidence / notes
CN-01	Consent is captured as a free, specific, informed, unconditional and unambiguous act with clear affirmative action (no pre-ticked boxes).	Act s.6(1)	CRITICAL	☐		*No silent/inferred consent*
CN-02	Each consent record is tied 1:1 to a specific purpose; granular opt-in per purpose, never a single bundled 'I agree'.	Act s.6(1); Rule 3	CRITICAL	☐		*Per-purpose ledger entry*
CN-03	Consent log captures, per entry: principal ref, purpose, data categories, notice version shown, timestamp, channel, and consent artefact.	Rule 6; Second Schedule	CRITICAL	☐		*Append-only ledger*
CN-04	Log is tamper-evident and append-only (hash-chained / signed) so any alteration is detectable on audit.	Rule 6 (integrity)	HIGH	☐		*SilicaSecure CMP ledger*
CN-05	Withdrawal of consent is logged as a first-class event and is as easy as granting; downstream processing stops on withdrawal.	Act s.6(4)–(6)	CRITICAL	☐		*Propagate stop-signal*
CN-06	On withdrawal, trigger cessation + erasure of data no longer supported by a lawful basis, and notify processors.	Act s.6(6), s.8(7)	HIGH	☐		*Wired to erasure job*
CN-07	Retain consent and related traffic/log records for at least one year (or longer if law requires).	Rule 6	HIGH	☐		*Retention policy set to ≥1yr*
CN-08	If using a registered Consent Manager, integrate with its interoperable APIs and honour its consent-artefact format.	Act s.6(7)–(9); Rule 4; Sched II	HIGH	☐		*Phase II: from 13 Nov 2026*
CN-09	Re-consent / refresh flow exists for purpose changes; new purpose = new notice + new consent, never silent expansion.	Act s.5, s.6	HIGH	☐		*Change-of-purpose trigger*
CN-10	Provide the Data Principal a self-serve consent dashboard to view, review and revoke active consents per purpose.	Act s.6(7); Rule 13	MEDIUM	☐		*Preference centre*
CN-11	Consent requests made via a Consent Manager / on behalf flows record the requester and basis for audit.	Sched II Part B	MEDIUM	☐		*Delegation trail*

Domain B — 11 controls. Mark Done only with evidence captured.

C Data Principal rights-request processes

Access, correction, erasure, grievance, nomination — intake to closure — Act s.11–14 / Rule 13.

ID	Checklist item / control	DPDP reference	Priority	Done	Owner	Evidence / notes
DR-01	Publish a single, discoverable channel (portal/email) for all rights requests, linked from every notice and the website.	Act s.13; Rule 13	CRITICAL	☐		*Rights intake portal*
DR-02	Right to access: return a summary of personal data processed and the identities of processors/fiduciaries it was shared with.	Act s.11	CRITICAL	☐		*Access-request workflow*
DR-03	Right to correction, completion and updating: workflow to amend inaccurate/incomplete data and push corrections to processors.	Act s.12(1)	HIGH	☐		*Correction + propagation*
DR-04	Right to erasure: delete personal data on request unless retention is legally required; confirm completion to the principal.	Act s.12(3)	HIGH	☐		*Erasure orchestration*
DR-05	Right of grievance redressal: ticketed mechanism with SLA tracking; respond within the period you publish (align ≤90 days).	Act s.13; Rule 13	CRITICAL	☐		*SLA clock + escalation*
DR-06	Right to nominate: capture and honour a nominee to exercise rights in event of death or incapacity.	Act s.14	MEDIUM	☐		*Nominee field + process*
DR-07	Identity-verification step proportionate to the request, without collecting excess data to verify.	Act s.6, s.13	HIGH	☐		*Verify without over-collecting*
DR-08	Define and publish reasonable response timeframes for each right; log received-date and closed-date per request.	Rule 13	HIGH	☐		*Timeframe register*
DR-09	Escalation path: if no/late response, principal can approach the Data Protection Board — document this in the response.	Act s.13(3)	MEDIUM	☐		*Board referral text*
DR-10	Rights requests routed to data processors via contract so they action access/correction/erasure within agreed SLAs.	Act s.8(2); Rule 6	HIGH	☐		*DPA clause + ticket relay*
DR-11	Maintain an auditable rights-request log (type, principal ref, dates, outcome) as compliance evidence.	Rule 6	HIGH	☐		*DSAR register*

Domain C — 11 controls. Mark Done only with evidence captured.

D Children's & disabled-persons' data

Verifiable parental/guardian consent and processing restrictions — Act s.9 / Rule 10–11.

ID	Checklist item / control	DPDP reference	Priority	Done	Owner	Evidence / notes
CH-01	Detect when a Data Principal is a child (<18) and obtain verifiable parental/guardian consent before processing.	Act s.9(1); Rule 10	CRITICAL	☐		*Age-gate + VPC flow*
CH-02	Do not undertake tracking, behavioural monitoring or targeted advertising directed at children.	Act s.9(3)	CRITICAL	☐		*Hard block in ad/analytics*
CH-03	Do not process children's data in a way likely to cause detrimental effect on their well-being.	Act s.9(2)	HIGH	☐		*DPIA for child journeys*
CH-04	For persons with disability, obtain consent of the lawful guardian where required.	Act s.9(1); Rule 10	HIGH	☐		*Guardian-consent path*
CH-05	Apply exemptions correctly (e.g., healthcare, education, child-transport classes) only where notified and documented.	Rule 11	MEDIUM	☐		*Exemption justification*

Domain D — 5 controls. Mark Done only with evidence captured.

E Retention, erasure & minimisation

Purpose-bound retention, Third-Schedule defaults and pre-erasure notice — Act s.8(7) / Rule 8.

ID	Checklist item / control	DPDP reference	Priority	Done	Owner	Evidence / notes
RT-01	Define a purpose-specific retention period for every data category; data is erased once the purpose is served.	Act s.8(7); Rule 8	CRITICAL	☐		*Retention schedule*
RT-02	Apply Third-Schedule defaults to specified classes (e.g., e-commerce/social media/gaming with ≥2 crore users: erase 3 yrs after last interaction).	Rule 8; Third Schedule	HIGH	☐		*Class check*
RT-03	Send the Data Principal advance intimation at least 48 hours before erasure where required.	Rule 8	HIGH	☐		*Pre-erasure notice job*
RT-04	Automate erasure/anonymisation jobs across primary stores, backups, logs and processors; record completion.	Act s.8(7); Rule 6	HIGH	☐		*Erasure orchestration*
RT-05	Data minimisation: collect only what each stated purpose needs; periodically prune dormant fields.	Act s.6(1)	MEDIUM	☐		*Field-level review*
RT-06	Accuracy: ensure data used for decisions affecting the principal is complete, accurate and consistent.	Act s.8(3)	MEDIUM	☐		*Data-quality controls*

Domain E — 6 controls. Mark Done only with evidence captured.

F Security safeguards & breach response

Reasonable safeguards, one-year logs and the 72-hour breach report — Act s.8(5)–(6) / Rule 6–7.

ID	Checklist item / control	DPDP reference	Priority	Done	Owner	Evidence / notes
SB-01	Implement reasonable security safeguards: encryption, masking/tokenisation, and virtual-token control over personal data.	Act s.8(5); Rule 6	CRITICAL	☐		*At rest + in transit*
SB-02	Access control + monitoring: least-privilege, logging of access/use, and detection of unauthorised access.	Rule 6	CRITICAL	☐		*SIEM use-cases*
SB-03	Retain security logs and monitoring records for at least one year to enable investigation.	Rule 6	HIGH	☐		*Log retention ≥1yr*
SB-04	Maintain backups/continuity so personal data can be restored after a compromise.	Rule 6	HIGH	☐		*Tested restore*
SB-05	Breach response: on a personal-data breach, intimate affected Data Principals without delay with nature, consequences and mitigations.	Act s.8(6); Rule 7	CRITICAL	☐		*IR playbook*
SB-06	Notify the Data Protection Board without delay and submit the detailed breach report within 72 hours.	Rule 7	CRITICAL	☐		*72-hour clock + template*
SB-07	Run a tested incident-response plan with defined roles, evidence capture and post-incident review.	Rule 6	HIGH	☐		*Tabletop done*
SB-08	Contractually bind processors to equivalent safeguards, breach reporting and erasure obligations.	Act s.8(2); Rule 6	HIGH	☐		*DPA security exhibit*

Domain F — 8 controls. Mark Done only with evidence captured.

G Data-processor & vendor governance

Processor register, DPAs and cross-border transfer controls — Act s.8(2), s.16 / Rule 6, 14.

ID	Checklist item / control	DPDP reference	Priority	Done	Owner	Evidence / notes
VP-01	Maintain a register of all data processors and the personal data each handles on your behalf.	Act s.8(2)	HIGH	☐		*Processor inventory*
VP-02	Execute valid Data Processing Agreements covering security, breach reporting timelines, audits, sub-processing and erasure.	Act s.8(2); Rule 6	CRITICAL	☐		*DPA template signed*
VP-03	Assess each vendor's security and privacy readiness before onboarding and periodically thereafter.	Rule 6	HIGH	☐		*Vendor risk assessment*
VP-04	Flow rights requests, withdrawal and erasure signals down to processors within agreed SLAs.	Act s.8(2)	HIGH	☐		*Relay mechanism*
VP-05	Govern cross-border transfers: restrict transfer to any country/territory the Government restricts under the transfer framework.	Act s.16; Rule 14	MEDIUM	☐		*Watch notified list*

Domain G — 5 controls. Mark Done only with evidence captured.

H Governance, records & SDF obligations

DPO, audit-ready records, DPIA/audit duties for Significant Data Fiduciaries — Act s.8–10 / Rule 9, 12.

ID	Checklist item / control	DPDP reference	Priority	Done	Owner	Evidence / notes
GV-01	Appoint and publish a point of contact / DPO able to answer questions about processing.	Act s.8(9); Rule 9	HIGH	☐		*Named + reachable*
GV-02	Maintain records demonstrating compliance — notices, consents, DPAs, rights logs, breach reports — audit-ready.	Rule 6	CRITICAL	☐		*Evidence vault*
GV-03	If notified as a Significant Data Fiduciary: appoint a DPO based in India who reports to the Board of Directors.	Act s.10; Rule 12	HIGH	☐		*SDF trigger watch*
GV-04	SDF: conduct annual Data Protection Impact Assessment and independent audit; furnish required reports.	Act s.10(2); Rule 12	HIGH	☐		*Annual DPIA + audit*
GV-05	SDF: perform algorithmic / due-diligence assessment to verify processing does not risk Data Principal rights.	Rule 12	MEDIUM	☐		*Algo fairness review*
GV-06	SDF: comply with any data-localisation / restriction-on-transfer measures specified for SDFs.	Rule 12	MEDIUM	☐		*Localisation check*
GV-07	Run periodic staff training on DPDP obligations, notice/consent handling and breach response.	Rule 6 (org. measures)	MEDIUM	☐		*Annual training log*
GV-08	Track the phased deadlines and assign an owner per milestone (CM go-live, full compliance).	Rules 2025 schedule	HIGH	☐		*See timeline below*

Domain H — 8 controls. Mark Done only with evidence captured.

T Compliance timeline & sign-off

Phased milestones under the DPDP Rules, 2025 — assign an owner to each.

Milestone	Date	What must be true	Owner	Status
Rules notified / Board live	**13 Nov 2025**	DPDP Rules in force; Data Protection Board operational; online complaints accepted.		☐
Soft-enforcement / build year	**Through 2026**	Gap assessment closed; notice, consent-log and rights workflows built and tested.		☐
Consent-Manager provisions	**13 Nov 2026**	Consent-Manager registration framework live; integrate with CM interoperable APIs.		☐
Full compliance (hard date)	**13 May 2027**	All substantive obligations met — no grace period expected; enforcement begins.		☐

Assessment completed by	Reviewed / approved by	Date
Name & role	Name & role	DD / MM / YYYY

Prepared by SilicaSecure Private Limited as an operational aid. It summarises and reorganises obligations under the DPDP Act, 2023 and DPDP Rules, 2025 in the firm's own words and does not reproduce the statutory text. It is not a substitute for legal advice or for reading the Gazette notifications.