DPOCERTIFICATION.ORG · FREE RESOURCE · FULL DEPTH

DPDP Readiness Checklist — Full Workbook

8 modules · Governance through SDF · DPDP Act 2023 & Rules 2025

8 modules · Expand matching sections on DPOCertification.Org/resources

1. Governance & Board oversight

Section 10 SDF obligations, DPO independence, and quarterly Board reporting cadence.

Control	Evidence	Owner	Frequency	Status
DPO appointment & independence	Board resolution + reporting line to audit committee	Board / CHRO	Annual review	—
Privacy steering committee	Charter, membership, meeting minutes	DPO	Monthly	—
Policy register	Privacy policy, retention, BYOD, AI use	Legal	Quarterly	—
Training & awareness	Role-based LMS + phishing simulations	HR / DPO	Quarterly	—
Regulatory horizon scan	MEITY / DPB circular tracker	Legal / DPO	Monthly	—
Budget & tooling	Consent, discovery, DLP, TPRM line items	CFO / DPO	Annual	—

Board pack checklist

- Executive summary: open gaps vs last quarter
- Consent withdrawal rate & grievance SLA metrics
- Material breach register (even near-misses)
- Processor concentration risk (top 5 vendors)
- Cross-border transfer status & TIAs pending

2. Notice & transparency (Rules 3–4)

Itemised notice, language accessibility, and change-management when processing evolves.

Notice element	Requirement	Artifact	Owner	Status
Purposes of processing	Specific, not bundled	Notice v3.2 + diff log	Legal	—
Categories of personal data	Including inferred / derived	Data inventory map	DPO	—
Retention schedules	Per purpose, not blanket	Retention matrix	Legal	—
Rights & grievance contact	Officer name + channel	Published FAQ	Comms	—
Processor disclosures	Sub-processor list link	Vendor register excerpt	Procurement	—
Children processing	Rule 7 carve-out if applicable	Age-gating spec	Product	—

3. Consent management (Section 6)

Granular, withdrawable consent with audit trail — CMP integration and product flows.

Flow	Test case	Expected outcome	Owner	Status
First-party signup	Marketing opt-in separate from T&C	Distinct consent IDs logged	Product	—
Cookie / SDK banner	Reject all equally prominent	No pre-ticked boxes	Product	—
Consent refresh	Purpose change triggers re-consent	Block processing until refresh	DPO	—
Withdrawal	One-click in account + email link	Processing stops within SLA	Product	—
Consent proof export	Regulator / audit request	JSON bundle with timestamps	Engineering	—
Legacy consent migration	Pre-DPDP databases	Re-consent campaign plan	Marketing	—

CMP evaluation criteria (reference)

- DPDP-native purpose taxonomy & Hindi UI
- Webhook to CRM / CDP on consent change
- SDK coverage: web, iOS, Android, server-side
- Integration with discovery & ROPA tools (e.g. Complynz)

4. Data principal rights (Sections 11–14)

Access, correction, erasure, grievance — 30-day SLA and nomination support.

Right	Channel	SLA	Verification	Status
Access / summary	Portal + email	30 days	OTP + ID match	—
Correction	Self-serve + agent	15 days	Audit trail	—
Erasure	Except legal retention	30 days	Legal hold check	—
Grievance	Dedicated officer	30 days	Ticket numbering	—
Nomination	Form + verification	30 days	Death certificate workflow	—
Automated decision	Opt-out where applicable	15 days	Human review queue	—

5. Security safeguards (Section 8)

Encryption, access control, logging, and alignment with CERT-In directions.

Safeguard	Standard	Evidence	Owner	Status
Encryption at rest	AES-256 or equivalent	KMS policy + rotation log	CISO	—
Encryption in transit	TLS 1.2+	Certificate inventory	Infra	—
RBAC / least privilege	Quarterly access review	IAM export	CISO	—
Logging & SIEM	Personal data access logs	90-day retention minimum	SecOps	—
Pseudonymisation	High-risk analytics	Architecture diagram	Data eng	—
Backup & DR	RPO/RTO for PII systems	DR test report	Infra	—

6. Breach notification & response

72-hour Board pathway and Data Protection Board notification templates.

Stage	Action	Owner	Target time	Status
Detect & contain	Isolate affected systems	SecOps	0–4 hours	—
Assess harm	Principal count, data types	DPO + Legal	4–24 hours	—
Board notification	Material breach criteria	DPO ’ Board	72 hours	—
Principal communication	Plain-language notice	Comms	As required	—
DPB notification	Prescribed format	Legal	As required	—
Post-incident review	Root cause + CAPA	CISO	14 days	—

7. Processors, vendors & transfers

ROPA-linked DPA register, TPRM tiering, and Section 16 transfer safeguards.

Vendor tier	Due diligence	Contract clause	Review cycle	Status
Tier 1 — critical PII	On-site / SOC2 + DPDP DPA	Audit + breach notify	Annual	—
Tier 2 — moderate	Questionnaire + sample audit	Sub-processor approval	18 months	—
Tier 3 — low touch	Standard DPA addendum	Liability cap alignment	24 months	—
Cross-border	TIA + whitelist country	SCC / BCR equivalent	Per transfer	—
Sub-processor change	30-day notice to fiduciary	Register update	Event-driven	—

8. SDF programme & DPIA

Significant Data Fiduciary controls: DPIA cadence, audits, and certification readiness.

SDF control	Rule / section	Deliverable	Owner	Status
DPIA for new high-risk processing	Rule 9	Signed DPIA register	DPO	—
Data auditor engagement	Rule 10	Annual audit plan	Board	—
Consent manager certification	Rule 5	CMP audit report	Product	—
Children safeguards	Rule 7	Verifiable parental flow	Product	—
Publication of transparency report	Best practice	Annual transparency PDF	Comms	—