SANJEEV BHARDWAJ
Senmig GRC Technologies • DPDP / GDPR / SOC 2 advisory
grcsanmig.com
sanjeev1911@gmail.com

CHECKLIST • RISK SCORING • DPDP vs GDPR / SOC 2

DPDP Implementation Checklist

A working checklist for India's Digital Personal Data Protection (DPDP) Act & Rules — with ISO/IEC 27001 mapping, officer roles, consent flows, incident reporting and a top-10 self-assessment risk-scoring questionnaire.

Why this matters now
DPDP is **more exhaustive but less authoritative** than GDPR — and **heavily penal**: up to **Rs. 250 crore** per contravention. RBI deadlines pending **November 2026**; MIT-advised IC integration target **July 2026**.

1. Governance & officer roles

- Appoint **Data Protection Officer (DPO)** — required for Significant Data Fiduciaries (SDFs).
- Designate **Data Fiduciary** accountable owner & board sponsor.
- Establish **grievance redressal officer** and SLA (≤ statutory window).
- Constitute internal **data protection committee** with legal, IT, infosec, business.

2. Consent & notice

- Standalone, plain-language **notice** in English & 22 scheduled languages.
- Granular, purpose-bound, **itemised consent** capture.
- Easy **withdrawal** — same friction as giving consent.
- Consent register / artefact with timestamp & lawful-basis evidence.
- **Consent Manager** integration where applicable.

3. Data Principal rights

- Access, correction, completion, updation & **erasure** workflows.
- Nomination & rights on behalf of children / persons with disability.
- Grievance escalation to **Data Protection Board of India**.

4. ISO/IEC 27001 mapping (back-end & front-end)

- **A.5 Information security policies** → DPDP policy stack.
- **A.8 Asset mgmt** → personal-data inventory & classification.
- **A.9 Access control** → least-privilege for personal data stores.
- **A.10 Cryptography** → encryption at rest & in transit.
- **A.12 Operations** → logging, backups, change & vuln mgmt.
- **A.15 Supplier** → DPA / processor contracts & due diligence.
- **A.16 Incident mgmt** → breach detection & reporting hooks.

5. Vendor / processor controls

- Data Processing Agreements (DPAs) with all processors & sub-processors.
- Onboarding due diligence; ongoing assurance & audit rights.
- Cross-border transfer restrictions & whitelisting.

6. Incident & breach reporting

- 24×7 detection; defined **severity matrix** & runbooks.
- Notify **Data Protection Board** & affected principals — without delay.
- Root-cause analysis, evidence preservation, regulator pack ready.
- Post-incident review & control uplift; board reporting.

SANJEEV BHARDWAJ
Senmig GRC Technologies • DPDP / GDPR / SOC 2 advisory
grcsanmig.com
sanjeev1911@gmail.com

RISK SCORING • TOP-10 QUESTIONNAIRE

DPDP Risk Self-Assessment

Score each question 0 (not started) – 3 (fully embedded). Maximum = 30. Banding: **0–10** Critical • **11–20** Elevated • **21–27** Managed • **28–30** Audit-grade.

#	Question	Mapping	Score (0–3)
1	Have you appointed a DPO and Data Fiduciary owner with board approval?	ISO 27001 A.5 / A.6	[ ] 0 [ ] 1 [ ] 2 [ ] 3
2	Is your personal-data inventory complete, classified and current?	ISO 27001 A.8	[ ] 0 [ ] 1 [ ] 2 [ ] 3
3	Do all collection points use plain-language, itemised, withdrawable consent?	DPDP §6 / §7	[ ] 0 [ ] 1 [ ] 2 [ ] 3
4	Are notices available in English and applicable scheduled languages?	DPDP §5	[ ] 0 [ ] 1 [ ] 2 [ ] 3
5	Are Data Principal rights (access / correction / erasure) fulfilled within SLA?	DPDP §11–§13	[ ] 0 [ ] 1 [ ] 2 [ ] 3
6	Are processors covered by DPAs with audit & sub-processor controls?	ISO 27001 A.15	[ ] 0 [ ] 1 [ ] 2 [ ] 3
7	Is encryption at-rest and in-transit enforced for all personal data?	ISO 27001 A.10	[ ] 0 [ ] 1 [ ] 2 [ ] 3
8	Do you have a tested breach-response runbook with regulator notification flow?	ISO 27001 A.16 / DPDP §8(6)	[ ] 0 [ ] 1 [ ] 2 [ ] 3
9	Are cross-border transfers mapped, restricted and approved?	DPDP §16 / RBI	[ ] 0 [ ] 1 [ ] 2 [ ] 3
10	Is the programme reported to the board with a quantified risk score?	Governance	[ ] 0 [ ] 1 [ ] 2 [ ] 3
	Total / 30	Risk band	_____

DPDP vs. GDPR vs. SOC 2 — at a glance

Dimension	DPDP (India)	GDPR (EU)	SOC 2 (US)
Type	Statute + Rules — **exhaustive but less authoritative** than GDPR	Comprehensive regulation with extensive case law	Voluntary attestation against Trust Services Criteria
Maximum penalty	**Up to Rs. 250 crore** per contravention — **heavily penal**	Up to €20M or 4% of global turnover	No statutory fine; loss of attestation & commercial impact
Lawful basis	Primarily **consent** + limited legitimate uses	Six lawful bases incl. legitimate interests	Not basis-driven; control-driven
Cross-border	Negative-list approach via central government	Adequacy / SCCs / BCRs	Customer-defined; assessed via controls
Regulator	**Data Protection Board of India**	National DPAs + EDPB	AICPA framework; auditor opinion
Scope of breach reporting	Notify Board & principals without delay	72-hour notification to DPA	Per contractual & control commitments
Best-fit posture	Mandatory for India ops & Digital India push	Mandatory for EU data subjects	Expected by enterprise & investor due-diligence

Coverage: aligned with global data-protection authorities and applicable to scaling, investment-bound and regulated companies in India — fintechs, BFSI, NBFCs, HFCs, VDASPs and the broader Digital India push.