DPDP Act 2023
Compliance Checklist

A 20-point self-assessment for Indian businesses

Score each item: Done / Partial / Not started. More than 8 'Not started' = urgent-action zone.

1. Data Mapping & Inventory

You cannot protect what you do not know you have.

- ☐ 01 Documented inventory of all personal data (customer, employee, vendor) with source, purpose, retention.
- ☐ 02 Mapped where personal data flows — from collection, through systems, to third parties, to storage.
- ☐ 03 Classified personal data by sensitivity (financial, health, Aadhaar-linked, children) with controls.
- ☐ 04 Listed every vendor / SaaS receiving personal data with Processor vs. Sub-Processor role identified.

2. Consent Management

Free, specific, informed, unconditional consent — separate from T&Cs.

- ☐ 05 Explicit, purpose-specific consent before processing, with plain-language notice in relevant languages.
- ☐ 06 Mechanism for users to withdraw consent as easily as they gave it — systems that actually stop.
- ☐ 07 Auditable log of when and how each consent was obtained and later withdrawn.
- ☐ 08 Verifiable parental-consent workflow for minors; no targeted ads / behavioural monitoring on children.

3. Data Principal Rights

Users now have enforceable rights. Be ready to honour them.

- ☐ 09 Documented, tested process for access / correction / erasure with a published contact point.
- ☐ 10 Formal grievance-redressal mechanism with named owners and stated SLA (recommend: 7 days).
- ☐ 11 Nomination facility in case of Data Principal death or incapacity.

hello@ringsafe.in

4. Security Safeguards

Technical and organisational controls. Act says "reasonable"; regulators will say more.

- ☐ 12 MFA on every system that touches personal data — no exceptions for admin accounts.
- ☐ 13 Encryption in transit (TLS 1.2+) and at rest (database or field-level for sensitive attributes).
- ☐ 14 Least privilege — access reviewed quarterly and revoked on role change or exit.
- ☐ 15 Logging and monitoring that detects unauthorised access within hours, not weeks.

5. Governance & Accountability

Name the roles. Train them. Document decisions.

- ☐ 16 Appointed Data Protection Officer (or Contact Person) with a published channel.
- ☐ 17 Board-level data-protection review at least twice a year with minuted decisions.
- ☐ 18 Documented DPDP-awareness training for every employee handling personal data, within 12 months.

6. Breach & Incident Response

Breach notification is mandatory. Test the drill.

- ☐ 19 Written Incident Response plan covering personal-data breaches, with responders and templates.
- ☐ 20 Tested the breach-notification workflow in a tabletop within the last 12 months (72-hr window).

Need help implementing DPDP?

Book a free 30-min consultation — walk away with 3-5 specific actions.

ringsafe.in/contact · hello@ringsafe.in · +91 8527376636