CHECKLIST

DPDPA Readiness Checklist 2026

India's Digital Personal Data Protection Act — each obligation mapped to the action you take and the platform module that supports it: consent, notice, rights & grievance, 72-hour breach response, SDF duties, and DPO governance.

Published by
Compliance Enablers LLP

Last Updated
March 2026

Pages
~10 pages

Introduction

India's Digital Personal Data Protection Act, 2023 (DPDPA) is the country's first comprehensive, standalone data protection law. It governs the processing of digital personal data of individuals (Data Principals) located in India, and reaches organisations (Data Fiduciaries) anywhere in the world that process such data in connection with offering goods or services in India.

The Act centres on consent, notice, purpose limitation, and accountability, and introduces meaningful penalties of up to INR 250 crore for failure to implement reasonable security safeguards. Significant Data Fiduciaries (SDFs) — designated by the Government based on volume and sensitivity of data, risk to Data Principals, and other factors — carry additional duties including appointing a Data Protection Officer in India, conducting Data Protection Impact Assessments, and commissioning independent audits.

This checklist maps each major DPDPA obligation to the concrete actions you need to take, and to the platform capability that supports it. It is organised so you can use it as a self-assessment, a board-readiness brief, or a project plan. Every item is genericised and framework-driven — there is no client, audit, or engagement data here, only the obligation and how the platform helps you meet it.

Use the three columns conceptually: the **Obligation** (what the law requires), the **Action** (what you do), and the **Platform Module** (where the work lives in your GRC system).

1. Lawful Processing & Consent

DPDPA permits processing only with the Data Principal's consent or for certain "legitimate uses". Consent must be free, specific, informed, unconditional, and unambiguous, with a clear affirmative action — and as easy to withdraw as to give.

Obligation	Action	Platform Module
Obtain valid consent before processing	Implement an opt-in consent mechanism with clear affirmative action; no pre-ticked boxes or bundled consent	Consent Management
Maintain proof of consent	Record who consented, when, the purpose, and the notice shown at the time; keep an auditable consent log	Consent Management
Honour withdrawal of consent	Provide an easy withdrawal path and stop processing that relied on the withdrawn consent	Consent Management
Rely on legitimate uses correctly	Document where you process under a permitted legitimate use rather than consent, and record the justification	Records & Register
Identify lawful basis per activity	Map each processing activity to its lawful basis and review when purposes change	Data Mapping (RoPA)

- ☐ **1.1 Stand up a compliant consent capture flow** with affirmative, unbundled opt-in.
- ☐ **1.2 Log every consent event** with purpose, timestamp, and the notice version shown.
- ☐ **1.3 Build a one-click withdrawal path** and wire it to downstream processing.
- ☐ **1.4 Document legitimate-use processing** where consent is not the basis.

2. Notice to Data Principals

Every request for consent must be accompanied by, or preceded by, a clear and plain-language notice describing the personal data to be processed, the purpose, how to exercise rights, and how to complain to the Data Protection Board of India.

Obligation	Action	Platform Module
Provide a clear privacy notice	Publish a plain-language notice covering data, purpose, rights, and grievance routes	Privacy Notice
Offer the notice in accessible languages	Make the notice available in English and Indian languages as appropriate to your audience	Privacy Notice

Version and timestamp notices	Keep a history of notice versions so you can show what each Data Principal was told	Privacy Notice

- ☐ **2.1 Draft a DPDPA-aligned notice** covering data, purpose, rights, and the Board complaint route.
- ☐ **2.2 Provide language options** appropriate to your user base.
- ☐ **2.3 Version every notice** and link it to the consent it supported.

3. Data Principal Rights & Grievance Redressal

Data Principals have the right to access information about their data, to correction and erasure, to grievance redressal, and to nominate another individual to exercise rights in the event of death or incapacity. You must publish the contact details of a person who can answer questions about processing.

Obligation	Action	Platform Module
Handle access requests	Provide a summary of the data processed and the processing activities and recipients	DSR / Rights Requests
Handle correction and erasure	Correct, complete, update, or erase personal data on validated request	DSR / Rights Requests
Operate a grievance mechanism	Publish a grievance channel and respond within your stated, reasonable period	Grievance Redressal
Support nomination	Allow a Data Principal to nominate another individual to exercise their rights	DSR / Rights Requests
Verify requester identity	Verify identity proportionately before fulfilling a request	DSR / Rights Requests

- ☐ **3.1 Publish a rights-request intake** for access, correction, and erasure.
- ☐ **3.2 Operate a grievance channel** with tracked response times.
- ☐ **3.3 Support nomination** of an alternate rights-holder.
- ☐ **3.4 Verify identity** before fulfilling any request.

4. Personal Data Breach Response (72-Hour Mindset)

DPDPA requires Data Fiduciaries to notify both the Data Protection Board of India and each affected Data Principal in the event of a personal data breach, in the form and manner prescribed. Build your programme to detect, assess, and notify quickly — a "72-hour mindset" keeps you ahead of the prescribed timelines and aligned with parallel obligations such as CERT-In's incident reporting and the GDPR's 72-hour rule where you process EU data.

Obligation	Action	Platform Module
Detect and triage breaches	Run an incident pipeline that classifies severity and flags personal-data impact	Incident Management
Notify the Board	Prepare and send a breach notification to the Data Protection Board in the prescribed manner	Incident Management
Notify affected individuals	Notify each affected Data Principal with the nature, consequences, and mitigation	Incident Management
Maintain a breach register	Keep an auditable record of every breach, the timeline, and actions taken	Incident Management

- ☐ **4.1 Stand up an incident pipeline** that flags personal-data impact at intake.
- ☐ 4.2 Pre-draft Board and Data Principal notification templates.
- ☐ **4.3 Track every breach to a register** with a full timeline.
- ☐ **4.4 Rehearse the notification path** so you can move within 72 hours.

5. Significant Data Fiduciary (SDF) Duties

If the Government designates you a Significant Data Fiduciary, you take on enhanced obligations: appoint a Data Protection Officer based in India who reports to the board or governing body, appoint an independent data auditor, conduct periodic Data Protection Impact Assessments, and undertake periodic audits and other prescribed measures.

Obligation	Action	Platform Module
Appoint a DPO in India	Designate a DPO based in India reporting to the board; publish their contact	DPO Workspace
Conduct DPIAs	Run Data Protection Impact Assessments on higher-risk processing	DPIA / Assessments
Commission independent audits	Engage an independent data auditor and track findings to closure	Audit Management
Demonstrate accountability	Maintain evidence of governance, reviews, and decisions for the regulator	Evidence & Register

- ☐ **5.1 Confirm whether you may be designated an SDF** based on data volume and sensitivity.
- ☐ **5.2 Appoint an India-based DPO** reporting to the board.
- ☐ **5.3 Run DPIAs** on high-risk processing and track remediation.
- ☐ **5.4 Plan independent audits** and manage findings to closure.

6. Data Protection Officer & Governance

Whether or not you are an SDF, you must publish the contact details of a person able to answer questions about processing. Significant Data Fiduciaries must appoint a formal DPO in India. Good governance means a named owner, a clear reporting line, and a place where reviews, decisions, and evidence live.

Obligation	Action	Platform Module
Name a contact for queries	Publish a contactable person for processing questions	DPO Workspace
Establish a reporting line	For SDFs, ensure the DPO reports to the board or governing body	DPO Workspace
Govern with evidence	Keep a register of reviews, approvals, and accountability artefacts	Evidence & Register

- ☐ 6.1 Name and publish a processing-queries contact.
- ☐ **6.2 Define the DPO reporting line** to the board for SDFs.
- ☐ **6.3 Keep an accountability register** of reviews and decisions.

7. Security Safeguards & Children's Data

The Act requires "reasonable security safeguards" to prevent personal data breaches — failure here attracts the highest penalty tier. Processing of children's data requires verifiable parental consent and prohibits tracking, behavioural monitoring, and targeted advertising directed at children.

Obligation	Action	Platform Module
Implement reasonable safeguards	Apply technical and organisational controls and evidence them continuously	Controls & Risk
Obtain verifiable parental consent	Verify parental/guardian consent before processing a child's data	Consent Management
Restrict child-directed processing	Prevent tracking, behavioural monitoring, and targeted ads to children	Consent Management

- ☐ **7.1 Map "reasonable security safeguards"** to your control framework and evidence them.
- ☐ **7.2 Implement verifiable parental consent** for children's data.
- ☐ **7.3 Disable tracking and targeted ads** for users identified as children.

How the Platform Supports DPDPA

The Compliance Enablers platform brings consent, notice, rights requests, grievance redressal, breach response, DPIAs, audits, and an accountability register into one multi-tenant system. Sage, our AI assistant — built on

Anthropic Claude, with every interaction disclosed, audited, and governed — helps draft notices, summarise rights requests, and surface the right control mappings, while keeping a human in the loop for every decision. Because the platform is framework-agnostic, your DPDPA programme reuses the same evidence and controls you already maintain for ISO 27001, SOC 2, and GDPR.
