INDIA DATA PROTECTION COMPLIANCE ROADMAP – 2027

A practical readiness checklist for businesses, institutions, platforms and data-handling organisations

Prepared by Trident Legal | Legislative position reviewed as at 10 November 2026

Purpose of this guide

This checklist helps an organisation identify the data it handles, map the legal regimes that may apply, and prepare for phased implementation of the Digital Personal Data Protection Act, 2023 (DPDP Act) and Digital Personal Data Protection Rules, 2025 (DPDP Rules). It is an operational planning aid, not a certification of compliance or a substitute for advice on the organisation's facts.

Important status distinction

The DPDP Act and Rules have staggered commencement. Some institutional provisions are already in force; the Consent Manager provisions are scheduled after one year; most substantive duties are scheduled after eighteen months. The Gazette notifications bear the date 13 November 2025, while MeitY/PIB public records also use 14 November 2025. For operational safety, prepare ahead of the earlier calculated dates and check the latest Gazette before relying on a deadline.

1. Build your legal and data inventory

( ) Identify every business unit, website, mobile application, customer portal, HR system, CRM, payment channel, CCTV system, call centre, cloud platform and paper-to-digital workflow that collects or uses information about identifiable individuals.

( ) Record categories of personal data: identity and contact details, employee and applicant records, customer transactions, financial information, device identifiers, location data, health information, children's data and other sensitive or high-risk records.

( ) Map the full lifecycle: collection, purpose, source, consent or other legal basis, access, sharing, storage location, retention, deletion, backups and archival.

( ) Identify the organisation's role in each activity: Data Fiduciary (determines purpose and means), Data Processor (processes on behalf of another), or both in different arrangements.

( ) Map vendors and onward recipients, including cloud providers, payroll processors, analytics providers, marketing agencies, call-centre operators, SaaS platforms and AI vendors.

2. Identify the legal regimes that apply

Regime	Why it matters	Action
DPDP Act, 2023 and DPDP Rules, 2025	Core framework for digital personal data processed in India, including certain overseas processing linked to offering goods or services to individuals in India.	Map processing, notices, consent, rights, security, processors and retention.
IT Act, 2000 and SPDI Rules, 2011	Existing security and sensitive personal data requirements remain relevant during the transition, including until the notified repeal of section 43A takes effect.	Review privacy policy, reasonable security practices and handling of sensitive personal data.
CERT-In Directions, 28 April 2022	Separate cyber-incident reporting and ICT log-retention requirements may apply, including six-hour reporting for listed incidents and 180-day log retention within India.	Maintain incident escalation, CERT-In point of contact and secure logs.
Sector-specific rules	RBI, insurance, securities, telecom, health and other regulators may impose additional security, confidentiality, outsourcing or localisation requirements.	Create a sector-by-sector obligations register; do not assume DPDP replaces these rules.

3. Prepare the core DPDP controls

( ) Create clear, standalone privacy notices that identify personal data and specific purposes; provide a simple way to withdraw consent and exercise statutory rights.

( ) Review consent journeys so consent is free, specific, informed, unconditional and unambiguous, supported by a clear affirmative action. Separate optional uses from data genuinely necessary for the service.

( ) Document reliance on a permitted legitimate use or statutory exception; do not treat an exception as blanket permission for unrelated processing.

( ) Put valid written contracts in place with Data Processors. Allocate security, confidentiality, sub-processing, incident cooperation, deletion, audit support and return-of-data obligations.

( ) Implement access controls, encryption or masking where appropriate, monitoring, logs, backups, vulnerability management and tested incident-response procedures.

( ) Create a retention schedule that distinguishes purpose-based deletion from records that must be retained under another law. Ensure deletion instructions reach processors and backups are managed consistently.

( ) Establish a channel to receive and track requests for access, correction, completion, updating, erasure, grievance redressal and nomination.

( ) Publish required business contact information for privacy queries. A statutory Data Protection Officer is specifically required for a Significant Data Fiduciary; other Data Fiduciaries must provide an appropriate contact person.

( ) Review products and services involving children. Assess verifiable parental consent, age and identity checks, and restrictions on tracking, behavioural monitoring and targeted advertising, subject to applicable exemptions.

( ) Assess whether the organisation may be notified as a Significant Data Fiduciary. If so, plan for an India-based DPO, independent data auditor, periodic Data Protection Impact Assessments and data audits.

4. Prepare for incident reporting

A single event may trigger more than one reporting regime. Do not assume that notifying one authority automatically satisfies every other legal duty.

( ) Maintain a 24-hour internal escalation route for suspected loss, unauthorised access, ransomware, exfiltration, accidental disclosure and vendor incidents.

( ) Preserve evidence, system logs, access records, timelines, affected systems, data categories, containment steps and communications.

( ) Assess whether the event is a cyber incident reportable to CERT-In under its 2022 Directions. Listed incidents must be reported within six hours of noticing them; further information may be supplied later as permitted by CERT-In's FAQ.

( ) Prepare for DPDP Rule 7: affected Data Principals must be informed without delay, and the Data Protection Board must be intimated without delay, with detailed information within the prescribed 72-hour period, subject to the Rule's terms.

( ) Maintain a regulator and customer notification matrix for sectoral regulators, contractual counterparties, insurers and law-enforcement requests.

( ) Run tabletop exercises involving legal, IT, HR, communications, senior management and key processors.

5. Data sharing and AI training

MeitY's October 2026 document titled *Data Empowerment and Protection Architecture (DEPA) for AI Training* is marked 'Draft for Discussion'. It proposes a techno-legal approach using data exchange platforms, electronic contracts, secure data environments and differential privacy. It is not, by itself, a new binding statute or a substitute for the DPDP Act. Organisations considering AI training or institutional data sharing should:

( ) Record dataset provenance, source permissions, original collection purposes and contractual or statutory restrictions.

( ) Determine whether a dataset contains personal data, commercially confidential information, trade secrets, copyrighted material or third-party data.

( ) Do not assume de-identification, aggregation or secure computing alone resolves every consent, purpose-limitation, confidentiality or intellectual-property issue.

( ) Review the proposed DEPA framework and monitor any formal government adoption, sectoral pilot, consultation or regulatory instrument.

( ) Use specific data-sharing agreements defining permitted use, access, model outputs, security, audit rights, onward disclosure, retention, deletion and liability.

6. Suggested implementation calendar

Period	Priority
Immediately – November 2026	Complete data mapping; confirm roles; inventory vendors; identify sensitive and children's data; check Consent Manager provisions and monitor official Board registration arrangements.
December 2026 – February 2027	Approve privacy notices; revise processor contracts; establish consent withdrawal and rights workflows; test retention and deletion; align incident-response playbooks.
March – April 2027	Test security controls, breach escalation, multilingual notices, children's consent controls and grievance channels; conduct a gap assessment and management sign-off.
Before May 2027	Complete readiness for substantive DPDP duties scheduled after eighteen months from Gazette publication. Verify the latest Gazette and sector-specific directions before final sign-off.

7. Management sign-off

( ) An accountable executive and operational privacy lead have been assigned.

( ) Legal, IT, HR, procurement, product and business teams have reviewed the data map.

( ) Material gaps have owners, target dates and documented risk acceptance where relevant.

( ) Processor contracts, privacy notices and incident procedures have been approved.

( ) Evidence of training, testing, approvals and remediation is retained.

Important legal note

This checklist is a general planning resource prepared with reference to official materials available on 10 November 2026. It does not certify compliance, determine whether an organisation is a Data Fiduciary or Significant Data Fiduciary, or resolve sector-specific questions. Commencement dates and regulatory instruments should be checked against the latest Gazette and regulator publications before action is taken.

Primary references: Digital Personal Data Protection Act, 2023; G.S.R. 843(E), 13 November 2025; Digital Personal Data Protection Rules, 2025, G.S.R. 846(E); CERT-In Directions No. 20(3)/2022-CERT-In, 28 April 2022; MeitY DEPA for AI Training, Draft for Discussion, October 2026.