AMLEGALS
STRATEGIC LAWYERING

NOVEMBER, 2025

THE C-SUITE PLAYBOOK

DPDPA **READINESS & GOVERNANCE**

Vibe Data Privacy

Leadership Perspective

The Digital Personal Data Protection Act, 2023 and its accompanying Rules, which were recently notified on **13 November, 2025**, are more than a checklist of compliance obligations.

It represents a fundamental shift in how digital power is distributed, returning agency, choice, and control to the individual. As organisations adapt to this new paradigm, the real opportunity lies not just in meeting legal requirements, but in embracing a more respectful, transparent, and trust-driven model of data governance.

This moment is a chance to rebuild the digital world with accountability at its core, and those who recognise this early will lead the way.

DPDPA is bigger than compliance, it is a redistribution of digital power.

Anandaday Misshra
Founder & Managing Partner

Executive Summary

The Digital Personal Data Protection Act, 2023 (DPDPA) and its subsequent Rules are now in effect. For your organization, this is not merely a compliance hurdle, it is a strategic inflection point.

Non-compliance carries significant financial penalties (up to ₹250 crore per instance) and, more critically, risks irreparable damage to your brand, customer trust, and market position in India.

The DPDPA and its accompanying Rules fundamentally reshapes how you collect, process, and leverage the personal data of over a billion people in one of the world's largest digital markets, in a staggered, phase-wise manner.

This playbook provides a clear, actionable framework for you, the C-suite, to oversee and govern your DPDPA compliance program.

It moves beyond initial readiness to establish a sustainable, evidence-based governance model that integrates with your global privacy framework (including GDPR, CCPA, etc.).

Your approach should be built on three pillars:

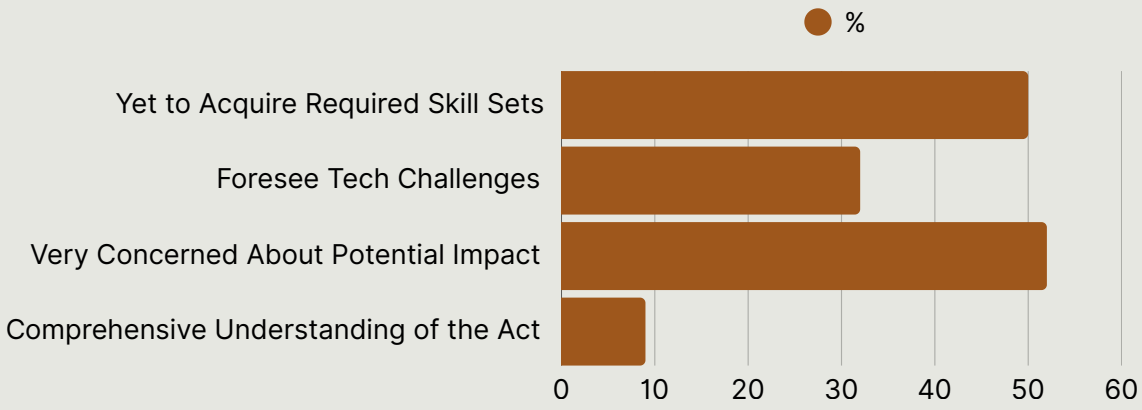
Accountability: Establishing clear ownership and accountability from the top down.

Transparency: Being explicit with your customers, employees, and partners about your data practices.

Trust: Using robust data protection as a competitive differentiator to build lasting customer loyalty.

This document outlines the core workstreams, a detailed checklist for each, and the "Evidence Pack" required to demonstrate compliance to the Data Protection Board of India (DPBI) and other stakeholders.

The C-Suite's Role: Ownership & Accountability



Source: EY, PWC

Practical Concerns that can be Addressed through C-Suite's Accountability

Chief Executive Officer (CEO):

- Accountability: Ultimate owner of the company's compliance posture and risk appetite.
- Action: Champion a "privacy-first" culture. Ensure DPDPA is a standing agenda item in board meetings. Allocate sufficient resources for sustained compliance.

Chief Financial Officer (CFO):

- Accountability: Assess and provision for financial risk associated with non-compliance.
- Action: Approve budgets for necessary technology, personnel, and consulting. Model the financial impact of potential penalties.

Chief Technology Officer (CTO) / Chief Information Security Officer (CISO):

- Accountability: Implement and maintain the technical and security measures to protect personal data.
- Action: Ensure your data architecture supports data minimization and purpose limitation. Oversee security safeguards (encryption, access controls) and the breach response protocol.

Chief Legal Officer (CLO) / General Counsel:

- Accountability: Interpret the law, oversee policy creation, and manage regulatory engagement.
- Action: Act as the primary advisor on DPDPA matters. Oversee contract remediation with data processors and manage interactions with the DPBI.

Chief Marketing Officer (CMO):

- Accountability: Ensure all marketing and customer engagement activities are DPDPA-compliant.
- Action: Overhaul consent collection for marketing communications. Use transparency in data practices as a brand-building tool.

Chief Human Resources Officer (CHRO):

- Accountability: Ensure the compliant processing of all employee and candidate personal data.
- Action: Update employment contracts, privacy notices for employees, and internal HR data handling policies as per the Rules.

The DPDPA Governance Checklist & Evidence Pack

This section forms the core of your ongoing governance program. For each workstream, you must track completion and maintain a corresponding Evidence Pack. The "Custodian" column is a suggestion and should be formally assigned within your organization.

Workstream 1: Governance & Accountability

Action	Status*	Custodian	Evidence Pack Component
Appoint Data Protection Officer (DPO) (if required) and Grievance Officer		CLO	• Formal DPO appointment letter/contract. • Formal Grievance Officer appointment letter/contract. • Publicly available contact details of the DPO and Grievance Officer.
Establish Privacy Steering Committee		CEO/CLO	• Committee Charter with defined roles, responsibilities, and meeting cadence. • Meeting minutes demonstrating regular oversight.
Develop/Update Master DPDPA Policy		DPO/CLO	• Version-controlled DPDPA Policy document. • Communication record showing policy distribution to all relevant staff.
Conduct Mandatory DPDPA Training		DPO/ CHRO	• Training materials (decks, videos). • Training completion logs and employee attestations.
Maintain Record of Processing Activities (ROPA)		DPO	An updated, comprehensive ROPA document (e.g., spreadsheet, privacy tool export) detailing data flows, purposes, retention, etc.

*Status entry by custodian.

As per reports, 52% of organisations are planning additional security controls around personal data but many have not started implementing, or have only partial understanding. Also CEOs / senior executives see compliance as both risk and opportunity (e.g. using trust & transparency as competitive advantage) in certain sectors.

Workstream 2: Lawful Processing (Notice & Consent)

Action	Status*	Custodian	Evidence Pack Component
Review All Data Collection Points		CMO/ CTO	Inventory of all forms, apps, and processes that collect personal data in India.
Draft & Deploy DPDPA-Compliant Notices		CLO/ DPO	• Standardized privacy notice templates. • Screenshots/records of notices deployed at each collection point.
Implement Granular Consent Mechanism		CTO/ CMO	• Screenshots/videos of the consent interface showing clear, specific, and freely given choices. • Technical documentation of the consent management platform.
Establish & Test Consent Withdrawal Process		DPO/ CTO	• A clear, accessible mechanism for users to withdraw consent. • Logs demonstrating successful processing of withdrawal requests within stipulated timelines.
Manage "Deemed Consent" Justifications		CLO	A legal register documenting every instance where "deemed consent" is relied upon, with clear justification (e.g., employment purposes, public interest).

82% of organisations believe that companies are not fully transparent (or only partially) in their data handling practices.

**Status entry by custodian.*

Workstream 3: Data Principal Rights Management

Action	Status*	Custodian	Evidence Pack Component
Establish a Data Principal Rights Portal/Process		DPO/ CTO	Publicly accessible webpage or email for submitting rights requests (access, correction, erasure).
Create Internal Workflow & Response Templates		DPO/ CLO	• Internal process flow diagram for handling requests. • Pre-approved response templates.
Implement Request Tracking System		CTO/ DPO	A log/dashboard of all requests received, their status, and time to resolution.

Workstream 4: Data Security & Breach Management

Action	Status*	Custodian	Evidence Pack Component
Implement "Reasonable Security Safeguards"		CISO/ CTO	• Information Security Policy documents. • Evidence of technical controls (e.g., encryption policies, access control logs, recent penetration test results).
Update Incident Response (IR) Plan for DPDPA		CISO/ DPO	The updated IR Plan specifically referencing DPDPA breach notification obligations to the DPBI and affected individuals.
Define Breach Notification Thresholds & Process		CLO/ CISO	• Internal guidelines defining what constitutes a reportable breach. • Draft notification templates for both the DPBI and Data Principals.

**Status entry by custodian.*

Workstream 5: Third-Party & Cross-Border Governance

Action	Status*	Custodian	Evidence Pack Component
Inventory All Data Processors Handling Indian Data		DPO/ Procurement	A centralized register of all third-party vendors (processors).
Remediate Contracts with DPDPA Clauses		CLO	• A standardized DPDPA Data Processing Addendum (DPA). • Tracker showing the status of DPA execution with all in-scope vendors.
Map All Cross-Border Data Transfers from India		CTO/ DPO	Data flow diagrams illustrating transfers of personal data outside of India.
Validate Legal Basis for Cross-Border Transfers		CLO	Legal analysis confirming that transfers only occur to countries on the central government's "whitelist" or meet other legal requirements.

**Status entry by custodian.*

Ongoing Governance & Board-Level Reporting

DPDPA compliance is not a one-time project.

Your Privacy Steering Committee should meet quarterly to review your compliance posture.

Your DPO (if appointed) should provide a report to the Board semi-annually, covering key metrics such as:

- **Data Principal Requests: Volume, type, and average time to resolution.**
- **Consent Management: Consent withdrawal rates vs. opt-in rates.**
- **Data Breaches: Number of incidents, time to detection, and time to notification.**
- **Training: Percentage of employees with up-to-date DPDPA training.**
- **Vendor Risk: Number of high-risk data processors and status of their compliance audits.**

This playbook should be reviewed and updated annually, or in response to any significant changes in the law or regulatory guidance.

AMLEGALS
STRATEGIC LAWYERING

Ready for India's biggest leap in data privacy?

Drop your thoughts at
dataprivacy@amlegals.com

Your Questions, Our Answers

+91-84485 48549 | +91-83478 53565

www.amlegals.com