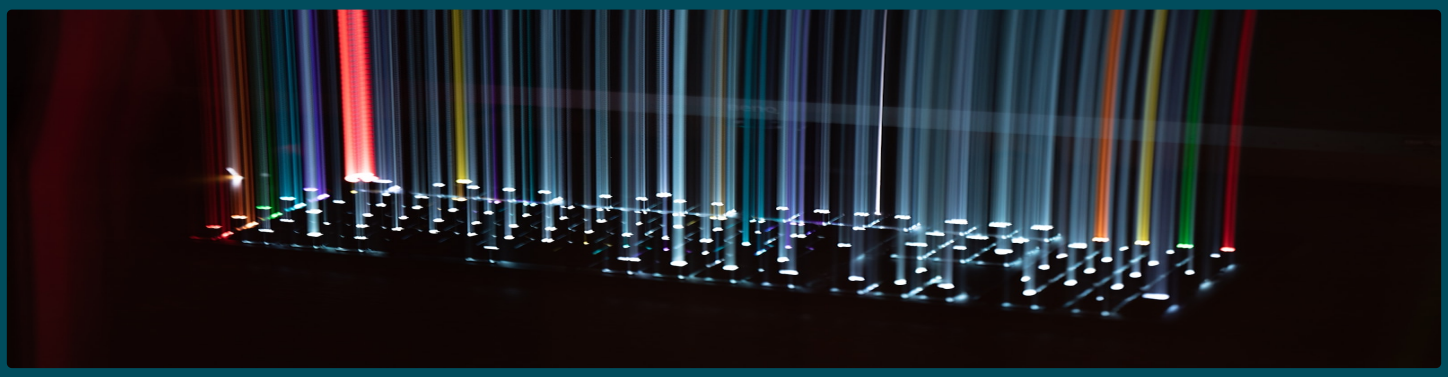
INDIALAW



DATA PRIVACY

Tightening The DPDP Screw: 12?Month Compliance Window On Government’s Radar

AUTHOR Appurv Bhatia

PUBLISHED 11 February 2026

India’s Digital Personal Data Protection (DPDP) law and its implementing rules set out a phased roadmap for organisations to align with new privacy obligations. Initially, companies were given up to **18 months** from notification to meet core requirements. However, the government is now exploring **shortening the DPDP compliance horizon to 12 months**, especially for larger players and significant data fiduciaries, creating an intensified regulatory push into 2026.

Table of contents

Industry Pushback Against Timeline Squeeze

Industry groups and digital associations have pushed back against proposals to compress the compliance window, warning that compressing an already tight transition period could strain technical, legal, and operational functions. Many organisations emphasise that thorough system redesigns, data?flow audits, and cross?functional change programs take time and that a rushed schedule could lead to security gaps and uneven implementation.

Top Focus Areas for Immediate Compliance

Whether the government retains the existing 18?month plan or shifts to an accelerated 12?month timeline, organisations should prioritise:

- **Consent mechanisms** – Move beyond generic privacy notices to purpose?specific, revocable, and auditable consent systems.
- **Retention discipline** – Clearly define lawful retention periods and automatically delete data that is no longer needed.
- **Breach preparedness** – Build and test incident response plans aligned with statutory breach notification timelines.
- **Governance for Significant Data Fiduciaries** – Embed risk assessments, accountability structures, and Data Protection Officer (DPO) roles.
- **Cross?border flow mapping** – Document cloud use, vendor arrangements, and overseas processing.

Immediate Action Plan: Day?1 Kickoff for Organisations

Assemble a cross-functional DPDP task force with executive buy-in today, allocating resources and setting weekly milestones to drive progress within the 12-month horizon.

Phase?1 (Weeks?1–4): Blitz Data Mapping and Audits

Start by cataloguing all personal data flows, where data is collected, processed, stored, and shared, and identify high?risk categories such as children’s data or international transfers.

Phase?2 (Weeks?5–12): Forge Consent and Retention Engines

Roll out granular consent systems that support easy withdrawal and automate retention expiry actions. Audit key third?party vendors to ensure they are aligned with DPDP norms.

Phase?3 (Months?4–6): Breach Drills and Governance Strengthening

Develop breach response playbooks, conduct table?top exercises, and solidify governance frameworks including annual risk assessments and DPO roles.

Phase?4 (Months?7–12): Scale, Test, and Certify

As the compliance deadline approaches, organisations should execute full system rollouts, conduct A/B tests on user journeys, validate breach responses, and embed privacy?by?design in new development efforts. Third?party audits and real?time monitoring dashboards will help catch gaps early, and cross?functional simulation tests will build organisational confidence ahead of certification or regulatory review.

Penalties for Non?Compliance: High Stakes Ahead

The DPDP framework carries significant financial penalties up to ?250 crore per instance, for non?compliance. Organisations can face fines running into crores of rupees for violations such as inadequate consent practices, excessive retention of personal data, or delayed breach reporting. Significant Data Fiduciaries, in particular, may face heightened scrutiny and enforcement measures, making early adherence both a legal requirement and a risk mitigation strategy.

Building DPDP Resilience: A Strategic Outlook Beyond Compliance

DPDP preparation should be treated not just as a regulatory checklist exercise but as an opportunity to elevate data governance and build long?term trust. Organisations can institutionalise privacy education, integrate ethical AI controls, and make continuous compliance a business asset.

Maintaining active engagement with government updates and industry forums will ensure organisations remain adaptive, turning what many see as a compressed timeline into a catalyst for deeper operational resilience and strategic data leadership.

For more details, write to us at contact@indialaw.in

References:

- **https://www.hindustantimes.com/india-news/industry-groups-asks-it-ministry-to-not-shorten-compliance-timeline-under-dpdp-101770233287416.html**

Related Practice Areas

Technology Law