KPMG

DPDP Act and Rules 2025

What is new for boards?



January 2026

Board Leadership Center (India)

KPMG. Make the Difference.

The Digital Personal Data Protection (DPDP) Act and Rules 2025 introduce one of India's first consolidated, enforceable framework for personal data governance. What is new is not the concept of privacy, but the explicit elevation of personal data to a board-visible governance responsibility.

The Act

Consolidates fragmented privacy obligations into a single regime,

Formalises accountability of organisations as data fiduciaries,

Establishes a dedicated data protection board,

and introduces enforceable penalties and directions.

For boards, this marks a shift from indirect awareness to demonstrable oversight. Personal data governance is no longer assumed to sit safely within IT or Legal functions—it is now an enterprise risk and trust issue.

DPDP Act readiness: What boards need to understand ?

The DPDP Act introduces personal data protection as a fiduciary obligation. It is not a narrow privacy statute, but a governance law requiring boards to exercise diligence in how data is collected, processed, safeguarded, shared, and retired. Boards are not expected to manage execution. They are expected to:

Understand the organisation's exposure,

Ensure accountability is assigned

and seek assurance that risks are identified and mitigated.







© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Why boards should be concerned ?

DPDP directly intersects with areas already under board oversight.

Area	Board implication
Regulatory risks	Penalties, enforcement actions
Reputational risk	Erosion of customer and employee trust
Operational risk	Business disruption due to breaches
Strategic risk	Constraints on AI, analytics, and growth
Accountability	Scrutiny of board awareness and response



Common transition risks observed across organisations

As organisations transition to the DPDP regime, several recurring risk patterns have emerged:

01 Assuming that consent alone ensures DPDP compliance

02 Over-reliance on 'legitimate use' without clear documentation

03 Incomplete data mapping, particularly across legacy systems and third parties

04 Limited visibility into vendor and cross-border data flows

05 Delayed breach detection and escalation

06 Treating data protection as a legal or IT issue rather than a governance responsibility.

These risks are typically structural, not intentional and therefore require board-level attention.

Key milestones and board commitments

November 2025

DPDPA Rules notified and Data Protection Board operational. This is the point at which boards should expect management to have clarity on scope, gaps, and execution plans.

November 2026

Consent manager registration deadline. Boards should require confirmation that consent infrastructure choices are finalised and compliant well ahead of this date.

May 2027

Full compliance required. All core obligations must be operational, tested, and evidenced. This should be treated as a firm internal deadline, not a regulatory aspiration.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

What boards are expected to oversee ?

01 Lawful grounds of processing

Boards should have assurance that personal data is processed on clearly defined lawful grounds:

- Consent (free, specific, informed, unambiguous), or
- Legitimate use, where permitted and justified.

02 Consent and privacy notice management

Boards should ensure that:

- Privacy notices are understandable and purpose-linked,
- Consent withdrawal is as easy as consent provision,
- Consent records are retrievable if challenged.

03 Accountability and governance

Boards should ensure:

- Clear ownership for DPDP compliance,
- Supporting policies and documentation,
- Regular reporting and escalation mechanisms.

04 Data principal rights and grievance redressal

Boards should seek assurance that:

- Rights requests (access, correction, erasure) are handled within timelines,
- Grievances are resolved effectively,
- Systemic issues are escalated.

05 Safeguards: Technical and organisational

Boards should ensure appropriate safeguards exist, proportionate to:

- Sensitivity of data,
- Scale of processing,
- Potential harm.

06 Data retention and disposal

Boards should satisfy themselves that:

- Personal data is retained only for defined purposes,
- Secure disposal mechanisms are operational.

07 Data breach preparedness

Boards should expect:

- Documented breach response playbooks,
- Clear escalation thresholds,
- Notification readiness for data principals and the Data Protection Board.



© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Cross-Border Data Transfers

Cross-border data transfers remain permitted, subject to evolving government conditions. Boards should maintain visibility over:

- **Where personal data is processed,**
- **Reliance on offshore vendors and cloud providers,**
- **Business continuity dependencies on overseas processing**

Cross-border data decisions should be viewed as governance risk decisions, not merely operational convenience choices.

DPDP Act readiness roadmap

Phase 1 Build	Phase 2 Implement	Phase 3 Manage
Establish the compliance foundation	Operationalise DPDP requirements	Sustain and demonstrate compliance
Conduct applicability and gap assessment across legal, technical, operational, and third-party dimensions.	Deploy consent management including age verification where required.	Establish continuous monitoring and management reporting.
Map and inventory personal data across systems, business units, cloud platforms, and vendors.	Implement workflows for data principal rights with defined service levels.	Conduct periodic independent and vendor audits.
Update notices, policies, contracts, and governance frameworks.	Define and enforce retention and disposal schedules.	Embed privacy by design into new initiatives.
Perform impact assessments for high-risk processing.	Strengthen technical and organisational safeguards.	Maintain auditable handling of data principal requests.
Develop a prioritised roadmap with ownership and timelines.	Update breach detection, response, and notification processes.	Regularly test breach preparedness through simulations and drills.
	Formalise processor controls through contracts and due diligence.	

Questions for Boards to consider under the DPDP regime

1. Does the board have assurance that personal data processing is lawful and documented?
2. Are consent mechanisms defensible if challenged?
3. Where does the organisation rely on legitimate use, and why?
4. Does the board have visibility into vendor and cross-border data dependencies?
5. Are grievance and rights mechanisms effective in practice?
6. Is the organisation prepared to respond to a data breach without delay?
7. Is DPDP oversight integrated with enterprise risk, cyber, and digital strategy?

Conclusion

The DPDP Act does not require boards to manage privacy operations. It requires them to ensure that personal data is governed with the same seriousness as financial, reputational, and strategic risk.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMG in India contacts:

Ritesh Tiwari
Partner
Board Leadership Center
E: riteshtiwari@kpmg.com

Nitin Shah
Partner, Digital Trust
Head, Cyber and Privacy
Strategy & Governance
E: nitinshah@kpmg.com

Shikha Kamboj
Partner, Digital Trust
National Leader, Data Privacy
and Ethics
E: skamboj@kpmg.com

kpmg.com/in

Access our latest insights on KPMG Insights Edge

Follow us on:
kpmg.com/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The views and opinions expressed herein are those of the quoted third parties and do not necessarily represent the views and opinions of KPMG in India.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai – 400 011
Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

This document is for e-communication only. (FL/BRO_0126_AC)