



DPDP Act 2023 and DPDP Rules 2025 simplified

From obligation to opportunity

Board Leadership Center (India)

December 2025

kpmg.com/in

KPMG. Make the Difference.



Interpreting the DPDP Act: Principles guiding our responsibilities

The DPDP Act, 2023 aligns with the universal privacy principles and adds India specific expectations around clarity, purpose discipline and accountable governance.

DPDP Act: Universal privacy principles

Lawfulness and purpose discipline	Use personal data only for clear, legitimate, well-defined purpose (e.g. KYC data for onboarding, risk and fraud checks) Secondary use of data will trigger consent and needs to be evaluated case basis (e.g. targeted marketing requires explicit consent)
Data minimisation	Collect only what is required for the stated purpose (e.g. asking year of birth instead of full DOB for eligibility checks)
Accuracy	Ensure decisions rely on correct, up-to-date information (e.g. updating contact details before sending notifications)
Retention limitation	Delete personal data once the purpose is fulfilled (e.g. removing applicant CVs after hiring cycles)
Security safeguards	Apply reasonable protections against unauthorised access or misuse (e.g. encrypting stored financial data like credit card numbers)
Transparency	Explain what is collected, why, who accesses it, and for how long (e.g. a clear notice before collecting health information)
Accountability	Be able to demonstrate governance, controls and audit trails (e.g. evidence of periodic compliance reviews).

DPDPA - Specific framework elements and expectations



SARAL standard

Simple, Accessible, Rational, Actionable

Privacy touchpoints must give people clarity and real control, without ambiguity or complexity.



Privacy based framework

The Act focuses on outcomes, not checklists

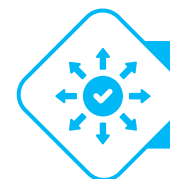
Organisations must show that their decisions and controls are reasonable and defensible.



Operational expectations

Ways of working

The rules define how compliance must work in practice, from breach timelines to consent design, retention controls and vendor oversight.



Lifecycle discipline

Controls must apply from collection to deletion

Each stage of the data journey needs clear purpose, security and accountability.

Together, these principles guide how we design controls, make decisions and demonstrate compliance under the DPDP Act.

From DPDP Act to action: Building organisational readiness

The act mandates organisations to establish robust governance frameworks anchored on four core pillars of responsibility. Each pillar sets out clear, enforceable standards for how personal data must be governed, managed, and safeguarded. These pillars define the foundation for compliance, risk mitigation, and trust in a data-driven environment.

Governance and leadership



- **Governance framework:** A formal structure for oversight, controls, issue escalation and reporting
- **Privacy Team:** Cross-functional group (legal, IT, HR/security) coordinating implementation
- **Data protection officer (DPO) :** Mandatory independent function for significant data fiduciaries (SDF)
- **Updated policies:** Privacy, retention, breach response and data handling policies aligned to the act
- **Vendor contract updates:** Adding requirements for breach notification, deletion and safeguards in vendor contracts
- **Training and awareness:** Building organisational understanding of privacy obligations
- **Audits/Compliance checks:** Periodic reviews of processes and controls by SDF
- **DPIA/Privacy risk assessment :** Evaluating high-risk processing for potential harm and documenting mitigation.

Data foundations



- **Data discovery:** Locating personal data across all systems, tools and teams
- **Data mapping:** Documenting how data flows between applications, processes and vendors
- **Records of processing:** Capturing what data is collected, for what purpose, where it is stored and who accesses it
- **Data classification:** Categorising data by sensitivity to apply appropriate safeguards
- **Retention schedule:** Defining how long each category of data should be kept
- **Deletion workflows:** Structured and auditable processes to remove data once purpose ends.

Rights and transparency



- **SARAL privacy notice:** Simple, accessible, rational, actionable disclosures explaining the collection, use and sharing, retention
- **Consent manager:** Optional system to capture consent, allow withdrawal and update preferences
- **Consent logs:** Timestamped proof of consent for audit and legal defense
- **Access requests:** Allowing individuals to view their data held about them
- **Correction requests:** Updating incorrect or outdated information
- **Erasure requests:** Deleting personal data when requested and permissible
- **Verification and closure:** Confirming identity and document communication
- **Appeal handling:** Escalation route when individuals contest responses.

Security and incident readiness



- **Security safeguards:** Encryption, access controls, MFA, monitoring, logging, configuration standards
- **Vendor controls:** Verifying that third parties meet required security privacy obligations
- **Breach identification and classification:** Recognising when an incident qualifies as a personal-data breach
- **CERT-In reporting (six hours):** Mandatory reporting to qualify cybersecurity incidents under CERT-In guidelines
- **Data protection board reporting (72 hours):** Mandatory notification of personal data breaches under DPDP Rules
- **Incident response workflow:** Defined steps for containment, assessment, notification and remediation
- **Evidence and logs:** Maintaining documentation for regular audits and internal review.

What the board needs to ask about DPDPA implementation?

To ensure readiness with the DPDP Act, the board must focus on strategic alignment, risk management, and accountability. These questions help identify gaps in governance and resource allocation. Asking the right questions ensures informed decisions and long-term organisational resilience.



How can we leverage DPDPA to strengthen trust and deliver a superior customer experience?

Focus on transparency, consent management, and personalised engagement while ensuring compliance.



What potential impact could DPDPA have on employee engagement and our internal culture of data responsibility?

Consider training, awareness, and fostering a privacy-first mindset.



In what ways will DPDPA influence our digital transformation roadmap and innovation initiatives?

Explore integration of privacy-by-design principles into new technologies and platforms.



How do our current cybersecurity practices position us for effective DPDPA compliance?

Assess alignment between existing security controls and regulatory requirements.



Will DPDPA introduce implications for our global operations, particularly in cross-border data transfers?

Evaluate restrictions, adequacy requirements, and contractual safeguards.



Who holds ultimate accountability for demonstrating compliance with DPDPA within our organisation?

Clarify roles of the board, senior leadership, and data protection officer.



Could DPDPA affect our strategic business partnerships and alliances?

Consider contractual obligations, shared data responsibilities, and risk exposure.



How will DPDPA reshape our vendor governance framework and operational oversight?

Examine due diligence, compliance certifications, and ongoing monitoring.

Now is the time to actively engage—challenge assumptions, demand clarity, and drive accountability for DPDPA readiness.

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 endeavour 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.

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.

© 2025 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.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.