WORKMATES

cloudworkmates.com

What's new in the DPDP Act Rules

Released on Nov 13, 2025

This is comparison of the Rules vs the DPDP Act released in August 2023.

BY: Ashish Mohanty
CISO, Workmates
Contributor to DPDP Act

WORKMATES

EFFECTIVE DATES & TRANSITION

The **Act:**

The Central Government may notify different commencement dates for different provisions, allowing staggered enforcement.

The **Rules:**

Rules 1, 2, and 17–21 are effective immediately from the Gazette publication date (Nov 13, 2025). Rule 4 (Consent Manager registration) comes into effect after one year from publication.
All other rules (3, 5–16, 22, 23) come into effect 18 months after Gazette publication.

Expert Opinion:

Government has given organizations 18 months to comply. The Effective date would be around Mid-May 2027. We think that the data protection board formation would start today, consent managers can register themselves around Mid-November 2026 and all the other rules are applicable from the effective date which would be around Mid-May 2027. This phased timeline offers organizations a practical runway for preparation without needing immediate overhaul, encouraging early establishment of core governance while allowing operational planning for the broader compliance requirements. This balance aids orderly implementation and risk mitigation.

Impact on Organizations:

Organizations must carefully map their compliance roadmap aligned with this phased timeline, starting immediate groundwork for governance and board engagement while preparing to operationalize consent management and full rule compliance nearer to the Mid-May 2027 deadline.

WORKMATES

NOTICE & CONSENT

The **Act:**

Requires a clear and concise notice to be provided before obtaining consent, and consent must be freely given with easy withdrawal options.

The **Rules:**

Demand detailed itemized notices explaining purpose, categories of personal data, and specific disclosures regarding third parties.
Set explicit withdrawal mechanisms that must be as easy as giving consent, including digital options like links/buttons for withdrawal.

Expert Opinion:

The rules in this domain has evolved a lot vs the Act. The notice and consent requirements are being made more prescriptive than almost any other domain in the act and rightfully so as the DPDP Act is a consent centric act. The notice and consent requirements in the rules make it clear about the implementation requirements and reduces the ambiguity on how one can read the act and the requirements which would avoid the confusion around it. The detailed prescriptions elevate compliance certainty while increasing the bar for technology and policy completeness necessary to ensure legitimate user control over data.

Impact on Organizations:

Organizations must invest in designing clear, transparent notices and robust technology platforms to support granular consent and immediate, uncompromised withdrawal workflows.

WORKMATES

CONSENT MANAGER

The **Act:**

Concept introduced, with the government empowered to notify rules for registration and operation.

The **Rules:**

Specify registration criteria including minimum net worth, fit and proper standards, and prohibition on reading stored data.
Set audit obligations and require the maintenance of a secure system that encrypts all consent data with strict access controls.
Require retention of consent records for seven years, ensuring traceability.

Expert Opinion:

The act defined the role of consent manager and the rules focused a lot more on operationalizing the role of consent manager. We are still on the fence about how consent managers would operate. Our questions are more around if there is a business case and a business model that can make consent manager role commercially viable. The other option that government may be thinking about is to have one of their own organizations as a consent manager. This would be an evolving domain. This creates both opportunities and uncertainties in the privacy ecosystem.

Impact on Organizations:

Organizations should proactively engage with emerging consent managers, evaluate risks and benefits of their role, and maintain operational flexibility to pivot as this market and regulatory approach develops.

WORKMATES

SECURITY SAFEGUARD

The **Act:**

Obliges reasonable security safeguards and breach notification requirements.

The **Rules:**

Mandate encryption of personal data in transit and at rest, role-based access control, and operational logs.
Require maintaining transaction logs for at least one year by default.
Set specific contractual clauses for processors, focusing on confidentiality and breach reporting.

Expert Opinion:

Security and privacy go hand in hand. The rules are so much more prescriptive around the security safeguards. We feel that the DPDP Act would not only force the organization to build privacy teams but it would have a major impact on security architecture of the organization. The prescriptive rules compel organizations to integrate privacy into foundational security design, enhancing risk coverage and regulatory confidence.

Impact on Organizations:

Organizations must enhance encryption practices, deploy granular access controls, implement detailed logging mechanisms, and update contracts with processors to meet these elevated security requirements.

WORKMATES

BREACH INTIMATION

The **Act:**

Data breaches must be notified to the Board and affected individuals as prescribed.

The **Rules:**

Stipulate that affected data principals be notified without undue delay, detailing breach nature, potential consequences, and mitigation measures.
Mandate Board reporting within 72 hours of becoming aware of the breach, including a
detailed report and follow-up updates.

Expert Opinion:

Data breach notification would require significant effort to operationalize. Till this point, organizations have had to notify the Cert-In but the requirements to notify the data principals would be a major effort. This puts greater emphasis on response timelines, communication clarity, and accountability which may require new cross- functional capabilities.

Impact on Organizations:

Organizations should build advanced incident response capabilities, formal communication plans for timely notifications, and staff training to comply efficiently with breach reporting duties.

WORKMATES

DATA RETENTION & ERASURE

The **Act:**

Requires erasure of personal data after the purpose is served or consent withdrawn, unless retention is legally mandated.

The **Rules:**

Provide that erasure must include a 48-hour prior notice to the data principal, explaining the timeline.
Impose a minimum one-year retention for logs related to data processing transactions and specify sector specific retention schedules.
Allow automated deletion unless data is retained for legal and compliance reasons.

Expert Opinion:

There are specific retention periods given for the given class of data fiduciaries. The question is would there be a similar retention period requirement specified for other sectors, we don't think so as of now. The other sectors would need to follow the law, define their own retention period, create retention schedules. The rules also specify the one-year retention of logs of data processing. There cannot be a clear indication that government expects you to know and track all the data processing activities.

Impact on Organizations:

Organizations should formalize sector-appropriate retention policies, implement automated deletion workflows and ensure transparent notification procedures preceding data erasure.

WORKMATES

CHILDREN & DISABLED - VERIFIABLE CONSENT

The **Act:**

Parental or lawful guardian consent is prerequisite for processing children's data.

The **Rules:**

Describe "verifiable consent" procedures, including identity verification via government- issued IDs or digital locker tokens.
Detail exceptions and specific conditions where tracking or processing children's data is permitted, with stringent safeguards.

Expert Opinion:

The Rules improve upon the Act by detailing verification techniques, reducing risk of unauthorized data access involving vulnerable populations. This layered approach promotes safety and accountability but also adds technical complexity, requiring organizations to have sophisticated verification tech or partnerships with trusted identity providers.

Impact on Organizations:

Organizations handling children’s or disabled persons’ data must implement rigorous identity verification measures and update privacy policies to reflect specified exceptions and protections.

WORKMATES

CHILDREN & DISABLED - VERIFIABLE CONSENT

The **Act:**

Requires DPO appointment, periodic audits, data protection impact assessments.

The **Rules:**

Mandate annual submission of Data Protection Impact Assessment and audit reports to the Board.
Require algorithmic due diligence to identify and mitigate tech-related privacy risks.
Include data localization mandates for certain sensitive data or processing under governmental direction.

Expert Opinion:

The enhanced regulatory scrutiny on significant fiduciaries will incentivize these entities to elevate governance maturity and embed privacy-by-design. Algorithmic risk assessments highlight the government's forward-looking approach recognizing AI/automation risks. Data localization brings operational and infrastructure implications but signals sovereignty priorities. It's a balancing act between regulatory compliance and innovation readiness.

Impact on Organizations:

Significant fiduciaries must enhance governance processes, embed algorithmic risk reviews in workflows, and review infrastructure to meet localization and audit mandates.

WORKMATES

CHILDREN & DISABLED - VERIFIABLE CONSENT

The **Act:**

Provides mechanisms for exercising personal data rights (access, correction, erasure, etc.) and nominating representatives.

The **Rules:**

Provide explicit digital procedures for rights exercise, including identity verification and authentication.
Set grievance redressal timelines, mandating a resolution or response within 90 calendar days. Define nomination procedures for representatives with detailed data necessary for processes.

Expert Opinion:

Digitization of rights exercise streamlines data principals' engagement and ensures standardized processes across fiduciaries. The grievance redressal deadline enforces accountability, pushing fiduciaries towards efficient complaint management systems. Nomination rights address continuity for incapacitated or deceased individuals, demanding sophisticated identity management.

Impact on Organizations:

Fiduciaries must implement digital rights management platforms, formal grievance processes, and secure representation nomination mechanisms to maintain compliance.

WORKMATES

CROSS-BORDER DATA TRANSFER RESTRICTIONS

The **Act:**

Government retains power to restrict cross-border data transfer via notifications.

The **Rules:**

Elaborate the process for imposing restrictions, requiring fiduciaries to conduct additional compliance steps before transfer.
Emphasize restrictions especially on significant fiduciaries for sensitive data categories, requiring localization or prior approval.

Expert Opinion:

There were a lot of rumours around the fact that there would be going to be restrictions on cross-border data transfer. The rules keep the status quo of the act and DPDP still makes it very easy to perform cross-border data transfer except negative list countries or as explained in the rules. This balanced approach preserves data flows critical to innovation while protecting national interests.

Impact on Organizations:

Organizations should maintain robust transfer compliance programs, monitor jurisdictional risks, and prepare to adapt data architecture if transfers are further restricted.