ManageEngine

A quick guide to the DPDP Act

The Digital Personal Data Protection Act, 2023 (DPDPA) is India's data privacy law, operationalized through the Digital Personal Data Protection Rules, 2025 and overseen by the Data Protection Board of India. It governs how organizations collect, process, protect, retain, and erase the personal data of individuals in India.

Technical controls checklist

Use the checklist below to assess your organisation's readiness across the DPDP Act and DPDP Rules, 2025 key requirement areas.

Sl.no	Requirement area	Article	Controls required
1	Access control and identity governance	Rule 6(1)(b)	• Enforce least-privilege access • Require MFA and SSO • Apply conditional access • Govern privileged accounts
2	Logging, monitoring, and review	Rule 6(1)(c)	• Centralize logs • Monitor data access • Audit directory changes • Certify access periodically
3	Backup and continued processing	Rule 6(1)(d)	• Back up directory data • Recover objects and attributes • Roll back after compromise • Contain ransomware
4	Log retention	Rule 6(1)(e)	• Retain logs one year • Archive logs securely • Keep records tamper-proof • Provide historical reports
5	Processor oversight	Rule 6(1)(f)	• Limit third-party access • Time-box processor sessions • Monitor processor activity • Apply approval workflows
6	Breach detection and intimation	Rule 7; § 8(6)	• Detect breaches in real time • Contain and isolate incidents • Reconstruct breach timelines • Generate breach evidence
7	Retention, erasure, and accuracy	Rule 8; § 8(3), § 12	• Erase data when purpose ends • Remove inactive accounts • Detect unauthorized changes • Support erasure requests

Source: www.meity.gov.in/data-protection-framework

The DPDP Act and ManageEngine

ManageEngine offers solutions that help organizations control access to personal data, monitor and audit how it is used, and detect and respond to breaches. AD360, ManageEngine's IAM solution, and Log360, its SIEM solution, together cover identity governance, security monitoring, backup, breach response, and data retention. With these, you can implement the technical controls required under the DPDP Act and the DPDP Rules, 2025.

How can ManageEngine help you implement the DPDP Act?

Data leak prevention

Block sensitive personal data from leaving the network via USB devices, email, printers, and cloud apps, and control high-risk endpoints to stop exfiltration.

Helps with Rule 6(1)(a)

Access and identity governance

Enforce least-privilege, role-based access and delegation, govern privileged accounts, and grant time-bound access to data processors.

Helps with Rule 6(1)(b); Rule 6(1)(f).

Multi-factor authentication

Require adaptive MFA, single sign-on, and conditional access for logons to the directories, applications, and endpoints that reach personal data.

Helps with Rule 6(1)(b).

Threat and integrity monitoring

Centralise and correlate logs, audit directory changes, monitor file integrity, and apply UEBA and MITRE-mapped detections to flag unauthorized access or changes.

Helps with Rule 6(1)(c); Section 8(3).

Access certification

Review who can reach personal data through periodic access certification and historical audit reports, supporting audits and impact assessments.

Helps with Section 10(2).

Backup and recovery

Back up Active Directory, recover objects and attributes granularly, and roll the directory back to a known-good state after compromise.

Helps with Rule 6(1)(d).

Log retention and archiving

Retain and securely archive logs for the one-year minimum, keeping records tamper-proof and available for investigation.

Helps with Rule 6(1)(e).

Breach detection and response

Detect breaches with real-time correlation and threat detection, contain them with automated playbooks, and reconstruct incident timelines for intimation.

Helps with Rule 7.

Retention and erasure

Erase personal data when its purpose ends, remove inactive accounts automatically, and keep tamper-proof records of every deletion.

Helps with Rule 8; Section 12.

For more information, contact sales@manageengine.com