Compliance Brief

THALES

CYBERSECURITY

Complying with India's Digital Personal Data Protection (DPDP) Rules 2025

cpl.thalesgroup.com

THALES

CYBERSECURITY

The Digital Personal Data Protection (DPDP) Rules, 2025, were announced by the Ministry of Electronics and Information Technology (MeitY) on November 13, 2025, which provide the operational framework for the DPDP Act, 2023, translating its broad legal principles into specific, actionable requirements for businesses, government bodies, and individuals.

Purposes

- Empowers Citizens: Gives "Data Principals" (individuals) granular control over their information.
- Ensures Accountability: Mandates that "Data Fiduciaries" (entities that collect data) follow strict security and transparency protocols.
- Digital-First Governance: Establishes a fully digital enforcement mechanism through the Data Protection Board of India.

Overview of DPDP Rules 2025

- Clear, itemized notices: Organizations must provide a simple, standalone list of what data is collected and why.
- Consent Manager framework: India based intermediaries let users manage, review, and withdraw consent across platforms from one dashboard.
- 72 hour breach reporting: Organizations must notify the Data Protection Board and affected individuals within 72 hours of a personal data breach, including impact and mitigation.
- Strict data retention and erasure: Personal data must be deleted once its purpose ends; large platforms must erase inactive user data after 3 years, with 48 hour prior notice.
- Protection for vulnerable groups: Verifiable parental consent is required for children's data, and targeted advertising or behavioral tracking of minors is banned.

Timeline (Phased Approach)

- Immediate (Nov 13, 2025): Launch of the Data Protection Board and key definitions.
- 12 months (Nov 13, 2026): Consent Manager registration and rules become enforceable.
- 18 months (May 13, 2027): Full compliance required for notice, consent, data erasure, and individual rights.

Penalties

- Not having "reasonable security safeguards" to prevent data breaches can lead to fines of up to 250 crore (about $30M+ USD).
- Failing to report a breach to the Data Protection Board can result in penalties of up to 200 crore.

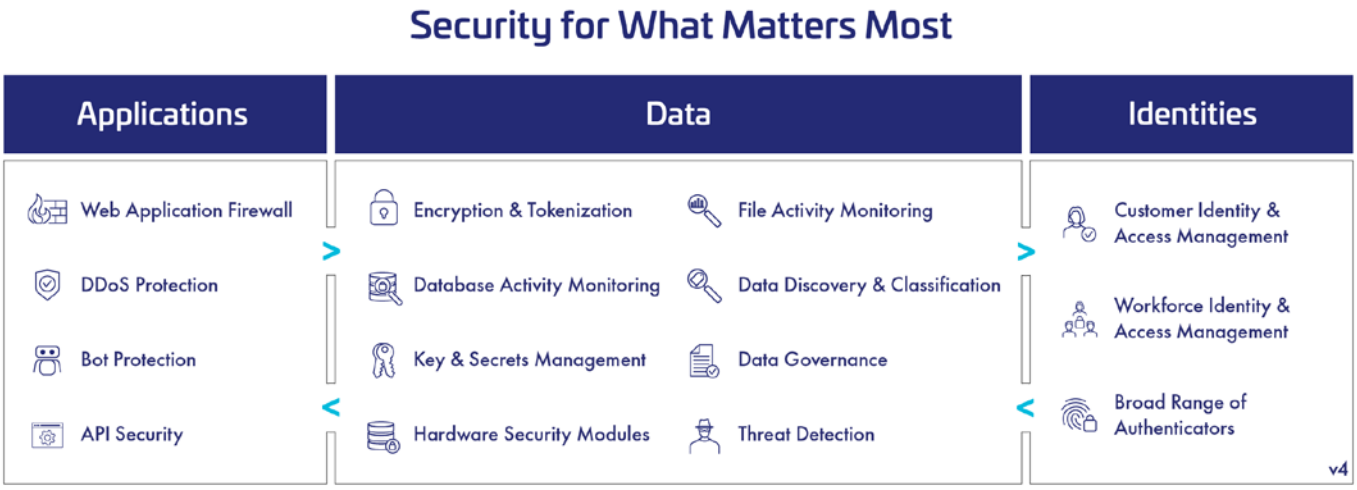
How Thales Helps with DPDP Rules Compliance

Thales' solutions can help organisations in India to address the seven rules in the DPDP Rule 2025 with a unified approach to data security and identity management.

DPDP Rule 2025	How Thales Helps	Solution Areas
Rule 4: Consent Manager & Rule 10: Verifiable Parental Consent Establishes the framework for managing consents and requires verifiable parental consent for children (minors).	• **Manage all users**, including the workforce, contractors, third-party users such as customers, suppliers, logistics, and B2B or B2C type users. • Create frictionless, secure, and **privacy-protected access** for your customers.	**Identity & Access Management** • Thales OneWelcome Identity Platform
Rule 6: Reasonable Security Safeguards Mandates technical and organizational measures to prevent data breaches, specifically mentioning encryption, masking, and access logs.	• **Identify** structured and unstructured **sensitive data** at risk on premises and in the cloud. • Identify the current state of compliance, document gaps, and **provide a path to full compliance**. • **Transparent and continuous encryption** protects against unauthorized access by users and processes in hybrid environments. • Provide a **unified visibility** of risks to critical data with a unique view of the strength of encryption for data across your entire data estate. • **Prevent unauthorized** access and alteration to its internals, including the audit logs. • **Pseudonymize sensitive information** in databases. • **Protect data in motion** with high-speed encryption. • Streamline key management in cloud and on-premises environments with **key lifecycle management**. • **Protect the root-of-trust** of a cryptographic system within a highly secure environment. • Enforce granular access control with transparent encryption for privileged users to prevent misuse or abuse. • **Manage system and data access rights** (access control) by supporting role-based authorization (**RBAC**) and conditional authorization (**ABAC**). • Control and manage **privileged user accounts** by supporting the enforcement of multi-factor authentication (MFA) for accessing critical systems. • Design authorization and approval procedures (User Journey Orchestration) **for privileged user accounts** and store and display as a privileged user activity report for detailed auditing.	**Data Security** • Application Data Protection • Data Activity Monitoring • Data Discovery & Classification • Data Risk Analytics • Enterprise & Cloud Key Management • Hardware Security Modules • High Speed Encryption • Transparent Encryption • Tokenization **Identity & Access Management** • Adaptive Access Control • Delegated User Management • Multi-Factor Authentication • Risk-Based Authentication • User Journey Orchestration

DPDP Rule 2025	How Thales Helps	Solution Areas
Rule 7: Intimation of Personal Data Breach Requires fiduciaries to notify the Board and individuals «without delay» (detailed report within 72 hours) and maintain an audit trail.	• Alert or block **database attacks** and abnormal access requests in real time. • **Monitor file activity** over time to set up alerts on activity that can put your organization at risk. • **Monitor active processes** to detect ransomware – identifying activities such as excessive data access, exfiltration, unauthorized encryption, or malicious impersonation of a user, and alerts/ blocks when such an activity is detected. • **Unify key management** operations with role-based access control and provide full audit log review.	**Data Security** • Data Activity Monitoring • Data Risk Analytics • Enterprise & Cloud Key Management • Hardware Security Modules • Transparent Encryption Ransomware Protection
Rule 8: Data Erasure & Retention Mandates the deletion of data once its purpose is served or after 3 years of inactivity (for certain entities).	• Ensure **secure deletion** by removing keys from CipherTrust Manager, digitally shredding all instances of the data.	**Data Security** • Key Management
Rule 13: Significant Data Fiduciary (SDF) Obligations Requires annual audits, Data Protection Impact Assessments (DPIAs), and advanced technical measures.	• **Classify and assign specific sensitivity levels** for data when you are defining your data stores and your classification profiles for different types of data sets. • Provide **real-time data dashboards** and reports.	**Data Security** • Discovery and Classification
Rule 15: Cross-Border Data Transfer Restricts or sets conditions for transferring personal data outside India.	• Secure sensitive data and **maintain complete governance** and control of sensitive data and the associated encryption keys and policies with Bring-Your-Own-Encryption (BYOE), Hold-Your-Own-Key (HYOK) and Bring-Your-Own-Key (BYOK) approaches, as well as a centralized multi-cloud key management. • Offer **transparent encryption** and access control for data residing. • **Encrypt sensitive data** once it is created and make sure cleartext data will not be processed or stored by unauthorized applications and personnel. • Allow root users to do their job without abusing data by **privileged user access controls**. • Accelerate threat detection and ease forensics with **data access audit logging**. • Employ **strong, standards-based encryption protocols**, such as the Advanced Encryption Standard (AES) for data encryption and Elliptic Curve Cryptography (ECC) for key exchange. • **Simplify key management** across on-premises and multi-cloud deployments by centralizing control on the FIPS 140-2 Level 3 environment. • Secure **data-in-transit** with future-proof encryption technologies to avoid "Harvest now, decrypt later".	**Data Security** • Cloud Key Management • Hardware Security Modules • High Speed Encryption • Tokenization • Transparent Encryption

Thales provides comprehensive cyber security solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.



Application Security: Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model. Our market leading product suite includes Web Application Firewall (WAF) protection against Distributed Denial of Service (DDoS) and malicious BOT attacks, security for APIs and a secure Content Delivery Network (CDN).

Data Security: Discover and classify sensitive data across hybrid IT and automatically protect it anywhere, whether at rest, in motion, or in use, using encryption, tokenization, and key management. Thales solutions also identify, evaluate, and prioritize potential risks for accurate risk assessment. They also identify anomalous behaviour and monitor activity to identify potential threats and verify compliance, allowing organizations to prioritize where to allocate their efforts.

Identity & Access Management: Provide seamless, secure, and trusted access to applications and digital services for customers, employees, and partners. Our solutions limit the access of internal and external users based on their roles and context with granular access policies and multi-factor authentication that help ensure that the right user is granted access to the right resource at the right time.

Organizations can leverage Thales' suite of identity, application and data security solutions available on a single unified platform to become compliant today and stay compliant in the future. Contact us now!

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.