Compliance Brief

Data Security Compliance with the India Digital Personal Data Protection Act, 2023

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

The Indian Parliament passed the Digital Personal Data Protection (DPDP) Act, 2023 in August 2023. The DPDP Act will replace Section 43A of the Information Technology Act, 2000 ("IT Act") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules"), which have been India's data protection framework until now. The DPDP Act is the first cross-sectoral law on personal data protection in India which is for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their data and the need to process such personal data for lawful purposes and matters connected therewith or incidental thereto.

Overview

The Act protects digital personal data (that is, the data by which a person may be identified) by providing for the following:

- The obligations of Data Fiduciaries (that is, persons, companies and government entities who process data) for data processing (that is, collection, storage or any other operation on personal data)
- The rights and duties of Data Principals (that is, the person to whom the data relates)
- Financial penalties for breach of rights, duties and obligations
- Establishment of Data Protection Board of India

Scope of the DPDP Act

The DPDP Act is 'principles-based legislation' that relies on concepts that are broadly similar to those in the GDPR. It governs data fiduciaries (i.e. data controllers), data processors and data principals (i.e. data subjects).

The DPDP Act applies to the following:

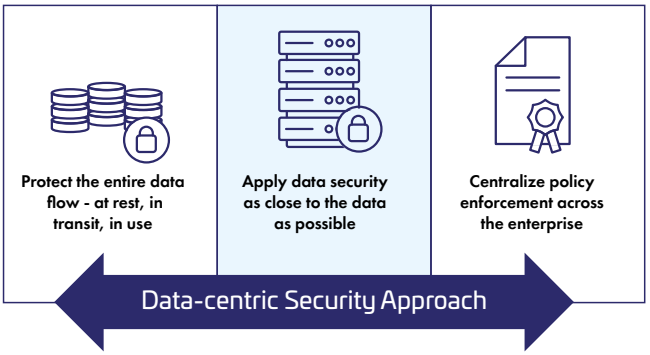
- Personal data capable of identifying the data principal, which is either collected digitally or is digitized after it is collected non-digitally.
- Personal data processed for personal or domestic purposes or aggregated personal data collected for research and statistical purposes which is not used for any decision specific to a data principal are excluded from the DPDP Act. Personal data made publicly available is also out of the scope of the DPDP Act.
- Data that is processed within Indian territory or, if processed outside, is in connection with any activity relating to the offering of goods and services to individuals within India.

Highlights of the Digital Personal Data Protection Act 2023

- It applies to the processing of digital personal data within India where such data is collected online, or collected offline and is digitized. It also applies to such processing outside India if it is for offering goods or services in India. The Bill allows the transfer of personal data outside India, except to countries restricted by the central government through notification.
- Personal data may be processed only for a lawful purpose upon consent of an individual. Consent may not be required for specified legitimate uses such as the voluntary sharing of data by the individual or processing by the State for permits, licenses, benefits, and services.
- Data fiduciaries will be obligated to maintain the accuracy of data, keep data secure, and delete data once its purpose has been met.
- It grants certain rights to individuals including the right to obtain information, seek correction and erasure, and grievance redressal.
- Government agencies are exempted from the application of provisions of the Bill in the interest of specified grounds such as security of the state, public order, and prevention of offenses.
- The central government will establish the Data Protection Board of India to adjudicate non-compliance with the provisions of the Bill.
- The Bill specifies penalties for various offenses such as up to: (i) Rs 200 crore for non-fulfillment of obligations for children, and (ii) Rs 250 crore for failure to take security measures to prevent data breaches. Penalties will be imposed by the Board after conducting an inquiry.

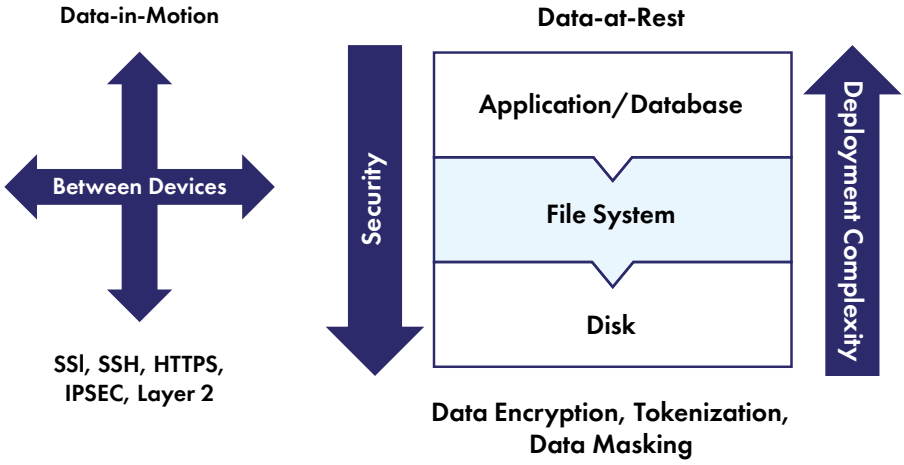
How can organizations prepare for it?

Thales offers a Data-centric Security approach to help organizations protect sensitive data and comply with **Digital Personal Data Protection Act** requirements. This approach focuses on protecting the data itself, regardless of its location, rather than just where it is stored. Data-centric security ensures that sensitive information is identified and protected with policy-based protection throughout the data lifecycle.



Encryption is a popular tool for securing **data in transit** and **at-rest** states. Organizations often choose to encrypt sensitive data before moving it or using encryptors to protect the contents of data in transit. For data-at-rest, enterprises can encrypt sensitive data in files and databases before storing them or the storage drive itself.

Enterprise security depends on strong **key management** and a separation of duties among different roles accessing sensitive data. Good key management systems can leverage a hardware-based root of trust, such as HSM, for key creation and storage.



Data-centric security gives organizations complete control over its sensitive data from the moment that each file or database record is created when it is properly implemented. Access to protected data can be granted or revoked at any time, and all activity is logged for auditing and reporting. Choosing a vendor with the broadest solution set available, as well as centralized key and policy management, will provide easier deployment and management controls when your organization grows.

What constitutes effective data security?

As one of the leaders in data security, Thales has helped hundreds of organizations comply with regulations worldwide by recommending the appropriate data security and identity management technologies required to meet regulatory requirements. The advanced data discovery, data encryption, key management, network encryption, hardware security module (HSM) and data protection on-demand solutions enable customers to protect and remain in control of their data wherever it resides – across cloud, on-premises and hybrid IT environments.

We trust that the best data security solutions provide an integrated suite of data protection capabilities, which allow organizations to gain greater visibility, use actionable insights, enforce real-time controls, and automate compliance support throughout the data protection journey. Some of the critical data protection capabilities are those in the diagram below.

Data Security

CipherTrust Platform unifies data discovery, classification, and protection and provides unprecedented granular access controls, all with centralized key management. You can rely on Thales **CipherTrust Data Security Platform** to discover, protect and control your organization's sensitive data, wherever it resides.

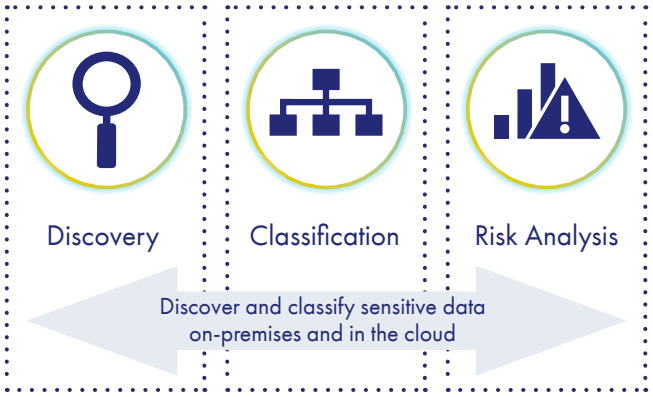
Data Discovery		Data-at-rest			Data-in-motion	Authentication
Data Discovery		**Centralized Key Management**		**Tokenization**		
	Data Classification		**Encryption**		**High-speed network encryption**	**Access Management and Authentication**

Discover

Data Discovery and Classification

The first step in protecting sensitive data is finding the data wherever it is in the organization, classifying it as sensitive, and typing it (e.g. PII, financial, IP, HHI, customer-confidential, etc.) so you can apply the most appropriate data protection techniques. Regular monitoring and assessment are crucial to prevent data breaches. **CipherTrust Data Discovery and Classification** efficiently identifies structured and unstructured data on-premises and in the cloud, supporting agentless and agent-based deployment models. It provides built-in templates for rapid identification, security risk identification, and compliance gaps, reducing remediation time and facilitating executive communication.

Data Discovery and Classification is the First Step in Effective Data Security



Data Activity Monitoring

Continuous monitoring captures and analyzes all data store activity, in the cloud or on-premises, for structured and unstructured data, for both application and privileged user accounts, providing detailed audit trails that show who accessed what data, when, and what was done to the data. **Imperva Data Security Fabric Data Activity Monitoring (DAM)** unifies auditing across diverse on-premises platforms, providing oversight for relational databases, NoSQL databases, mainframes, big data platforms, and data warehouses. It also supports databases hosted in Microsoft Azure and Amazon Web Services (AWS), including PaaS offerings such as Azure SQL and Amazon Relational Database Services (RDS). Detailed data activity is captured automatically, making it easier to fulfill audit requests.

Protect Data-at-Rest

Protect:

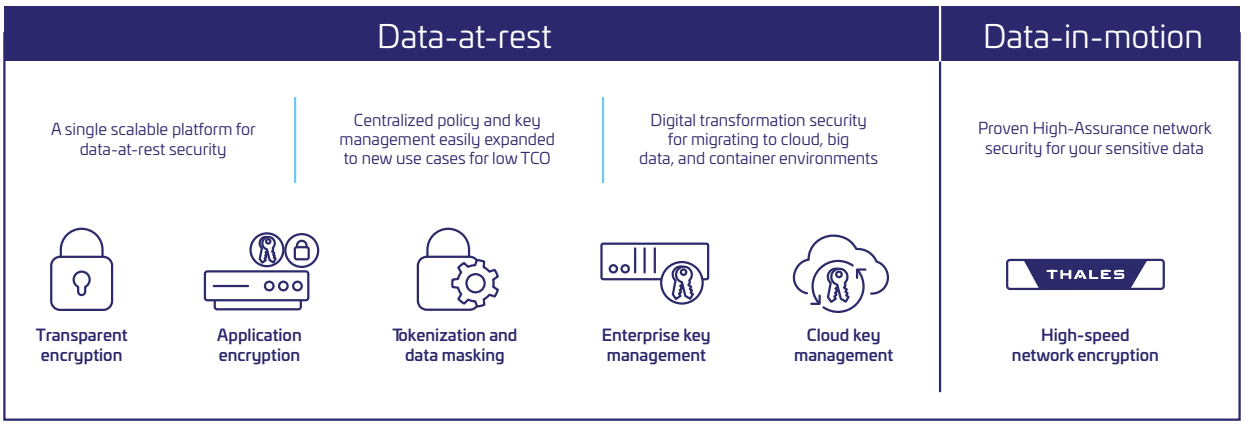
Once an organization knows where its sensitive data is, protective measures such as encryption or tokenization can be applied. For encryption and tokenization to successfully secure sensitive data, the cryptographic keys themselves must be secured, managed and controlled by the organization.

- **CipherTrust Tokenization** provides comprehensive data security capabilities, including file-level encryption with access controls, application-layer encryption, database encryption, static data masking, vaultless tokenization with policy-based dynamic data masking, and vaulted tokenization to support a wide range of data protection use cases.
- **CipherTrust Data Protection Gateway (DPG)** offers transparent data protection to any RESTful web service or microservice leveraging REST APIs. DPG is deployed between the client and web service and transparently protects sensitive data inline without modifying legacy or cloud-native applications. DPG interprets RESTful data, performs data protection operations based on policies defined centrally in Thales's CipherTrust Manager.
- **CipherTrust Transparent Encryption (CTE)** delivers data-at-rest encryption with centralized key management, privileged user access control, and detailed data access audit logging. This protects data wherever it resides, on-premises, across multiple clouds and within big data, and container environments.
- **CipherTrust Security Intelligence** logs and reports streamline compliance reporting and speedup threat detection using leading SIEM systems. The solution allows immediate automated escalation and response to unauthorized access attempts and provides all the data needed to build behavioral patterns required to identify suspicious usage by authorized users.

Control:

Organizations need to control access to their data and centralize key management. Every data security regulation and mandate require organizations to be able to monitor, detect, control, and report on authorized and unauthorized access to data and encryption keys.

- The CipherTrust Data Security (CDSP) Platform delivers robust **enterprise key management** via **CipherTrust Cloud Key Manager** across multiple cloud service providers (CSP) and hybrid cloud environments to centrally manage encryption keys and configure security policies so organizations can control and protect sensitive data in the cloud, on-premise and across hybrid environments.



- The **CipherTrust Data Security Platform** allows administrators to create a strong separation of duties between privileged administrators and data owners as well as to enforce very granular, least-privileged-user access management policies which can be applied by user, process, file type, time of day, and other parameters.
- Strong separation of duties policies can be applied to ensure one administrator does not have complete control over data security activities, encryption keys, or administration. In addition, the **CipherTrust Manager** supports two-factor authentication for administrative access.

Protect Data-in-Motion/ Transit

- **Thales High Speed Encryptors (HSE)** provide network-independent, data-in motion encryption (layers 2, 3, and 4) ensuring data is secure as it moves from site-to site, or from on-premises to the cloud and back. It allows customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception— without performance compromise. Thales HSEs are available as both physical and virtual appliances, supporting a wide spectrum of network speeds from 10 Mbps to 100 Gbps.

Strong Authentication and Access Management

Thales OneWelcome identity & access management solutions provide both the security mechanisms and reporting capabilities organizations need to comply with DPDP requirements. Our solutions protect sensitive data by enforcing the appropriate access controls when users log into applications that store sensitive data. By supporting a broad range of authentication methods and policy-driven role-based access, our solutions help enterprises mitigate the risk of a data breach due to compromised or stolen credentials or through insider credential abuse. Support for smart single sign-on and step-up authentication allows organizations to optimize convenience for end users, ensuring they only need to authenticate when needed. Extensive reporting allows businesses to produce a detailed audit trail of all access and authentication events, ensuring they can prove compliance with a broad range of regulations.

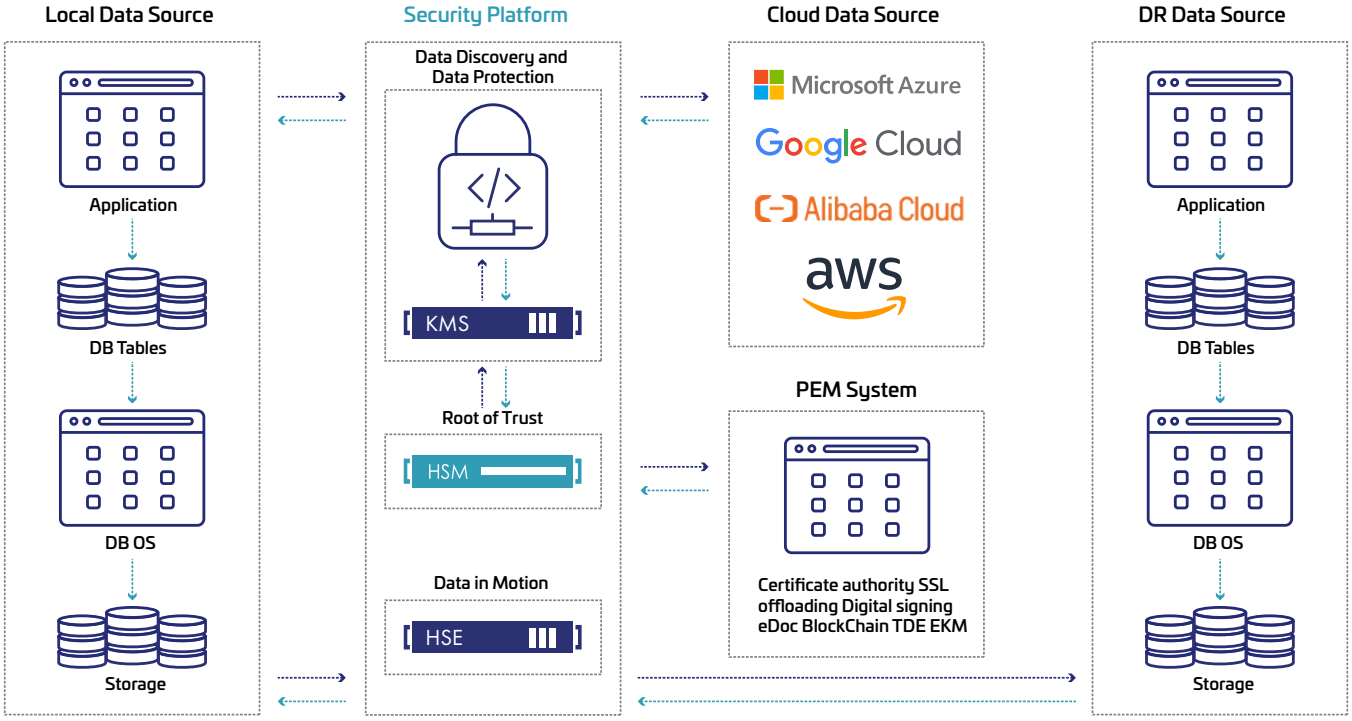


Image above: The Thales Cloud Protection & Licensing solutions in the above images consist of the following components:

√ Protect Data at Rest **√ Protect Data in Use** **√ Protect Data in Motion** **√ Secure Root of Trust**

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

About Thales

Thales is a global leader in data security, trusted by governments and the most recognized companies around the world to help them protect their most sensitive data. The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Thales Cloud Protection & Licensing

Data Protection

Access Management & Authentication

Software Monetization

#1

Worldwide in general-purpose HSMs

Worldwide in data encryption

Worldwide in payment HSMs

Worldwide in key management

Worldwide in cloud HSMs

Worldwide in cloud authentication

Worldwide insoftware protection

Worldwide in software licensing

2,600
Employees in 50+ countries

180
Countries where we sell our digital security solutions

750
Engineers worldwide

30,000
customers worldwide

Thales's technologies and services help secure **more than 80%** of all global payment transactions and increasingly valuable corporate and government information.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us