Solution Brief

Compliance with the Personal Data Protection Decree in Vietnam

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

The Vietnamese Government announced the Personal Data Protection Decree (Decree 13/2023/ND-CP) on April 17, 2023, and it comes into effect in July 2023. Before the issuance of the Decree, personal data protection in Vietnam was governed by 19 different laws and regulations, including general laws such as the Civil Code 2015 (November 24, 2015) and the Law on Cyber Information Security No. 86/2015/QH13 (November 19, 2015) ('LCS') and sectoral laws. The PDPD aims to fill these gaps in the fragmented legal framework and to provide a comprehensive and consistent approach to personal data protection, extending safeguards for personal data to over 97 million people in Vietnam.

In general, the protection of privacy and personal data is under the responsibility of the Ministry of Public Security (MPS). Other ministries, including the Ministry of National Defense, Ministry of Information and Communications, and Ministry of Science and Technology also have input on the MPS's decisions.

Scope of Personal Data Protection Decree (PDPD)

Personal Data Protection Decree (PDPD) applies to all individuals and entities operating in Vietnam who engage in the provision, collection, or utilization of data for any purpose within the country. This includes:

- Vietnamese agencies, organizations, and individuals;
- Foreign agencies, organizations, and individuals in Vietnam;
- Vietnamese agencies, organizations, and individuals operating abroad; and
- Foreign agencies, organizations, and individuals directly participating in or related to personal data processing activities in Vietnam.

Core principles

Personal Data Protection Decree 13/2023/ND-CP includes 44 articles marking a significant milestone in protecting personal data in the country.

- The Decree introduces key concepts and principles of personal data protection and sets out specific requirements for data processors and controllers.
- It establishes a regulatory framework for obtaining consent for data processing activities including the purchase and sale of personal information, as well as marketing and advertising, cross-border data transfers, and children data protection, which can contribute to safeguarding the privacy and security of individuals' personal data.
- Main categories of processing personal data of the Decree

1. Consent:

Organizations need to obtain the consent of the data subject before processing personal data. Such consent must be given expressly, voluntarily, and in full knowledge and in a format capable of being printed or copied in writing. An exemption applies under emergency circumstances to protect the life or wellbeing of the data subject or another person, or where personal data is processed by state authorities in accordance with applicable laws.

2. Rights of data subjects:

Data subjects must be notified about, among other things, the type of personal data that are collected, the purpose of collection and organizations that have access to the data, the amendment, deletion and destruction of their personal data. The data subject also has the right to claim damages, initiate legal proceedings, and implement measures for self-protection.

3. Protective measures:

Every organization needs to declare the internal regulations on personal data protection in line with PDPD requirements and the ability to delete personal data within a 72-hour window. The PDPD provides a high level of protective measures applicable when an organization needs to process sensitive data and children's data.

4. Impact assessment:

PDPD requires organizations to prepare and submit to the MPS an impact assessment record relating to their data processing activities. The record will be reviewed by the MPS and must be updated from time to time by the submitting entities upon any change to its content or upon request of the MPS.

A separate impact assessment is also required if the personal data of Vietnamese citizens is transferred abroad and if a location outside of Vietnam is used to process the data of Vietnamese citizens (a "cross-border transfer"). Organizations must submit an impact assessment record to the MPS within 60 days from the start of the transfer and must update such record from time to time upon any change to its content or upon the request of the MPS.

5. Reporting:

When a data breach or other violation of the PDPD occurs, the personal data controller and the personal data controller cum processor are obliged to notify the MPS of the incident (including the measures taken to minimize the incident's consequences) using the form provided by the PDPD within 72 hours.

When cross-border data transfer takes place, organizations must inform the MPS of information on the transfer and the contact details of the organizations or individuals in charge. Additionally, the MPS has the right to inspect a cross-border transfer once a year and may require the transferor to stop the transfer if (i) the relevant data is being used to infringe upon the national security

interests of Vietnam; (ii) the transferor fails to comply with relevant impact assessment and reporting requirements; and (iii) there has been a leak or loss of personal data of a Vietnamese citizen.

6. Penalties:

Non-compliance with PDPD can be subject to disciplinary action, administrative penalties, or criminal prosecution, depending on the severity of the violation.

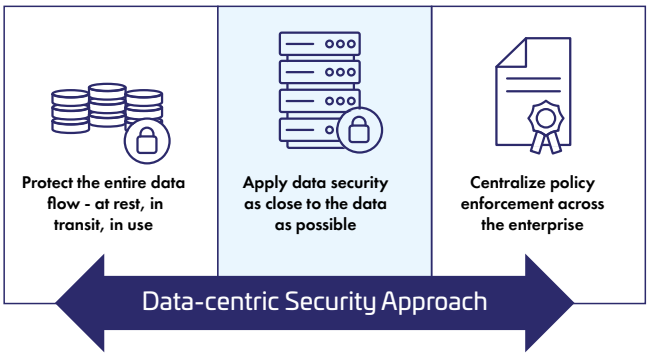
The Decree is in effect on July 1, 2023, giving organizations only two months to make the necessary adjustments to their business and operations to comply with the new regulations.

How can organizations prepare for it?

Address Personal Data Protection Decree (PDPD) with Data-centric Security Approach

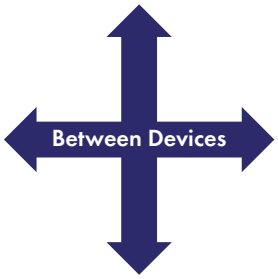
Thales can help organizations to protect sensitive data and to comply with Personal Data Protection Decree requirements with a Data-centric Security approach.

A data-centric security approach is integral to every worldwide data compliance regulation and is a foundational best practice. The defining characteristic of data-centric security is that **protection is applied to the data itself**, independent of the data's location.



Unfortunately, most data security technology focuses on protecting where data is, rather than the data itself—for example, protecting the data stored on a laptop or server, or all the data that crosses a specific network. The problem with this approach is that another solution is required as soon as data moves somewhere else, or data is left unprotected. Data-centric security, on the other hand, focuses on what needs to be protected – the files containing sensitive information – and applying the appropriate form of protection no matter where the data happens to be. To be effective, data must be protected automatically; sensitive information should be identified as soon as it enters an organization's IT ecosystem and should be secured with policy-based protection that lasts throughout the data lifecycle.

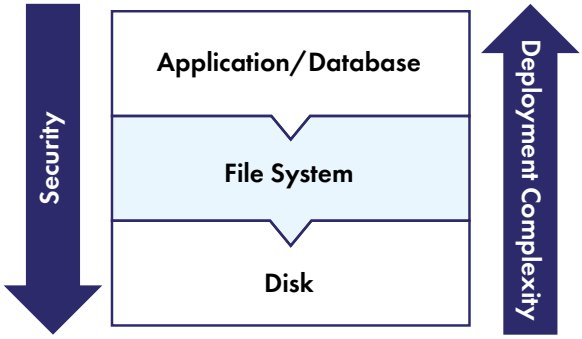
Data-in-Motion



SSl, SSH, HTTPS, IPSEC, Layer 2

Protection requires as data can be exposed to risks in both transit and at-rest states. As such, there are various approaches to protecting data in transit and at rest. Encryption is one of the popular tools and plays a major role in data security for securing data both in transit and at rest. Organizations often choose to encrypt sensitive data prior to moving it and/or use encryptors to protect the contents of data in transit. For protecting data-at-rest, enterprises can simply encrypt sensitive data in files and databases prior to storing them and/or choose to encrypt the storage drive itself.

Data-at-Rest



Data Encryption, Tokenization, Data Masking

Once an organization uses encryption technologies to safeguard its data, enterprise security then depends on the encryption key and policy management. Best practice data security solutions using cryptographic keys include strong key management and a separation of duties among different roles accessing sensitive data. Good key management systems will also provide the ability to leverage a hardware-based root of trust such as HSM for key creation and storage.

Data-centric security gives the organization 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. To properly execute your data-centric security approach, it's important to note the encryption and data protection methods that are available, the requirements, the applications or data to be protected, and the reasons for applying the chosen protection method. 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 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**

Data Security

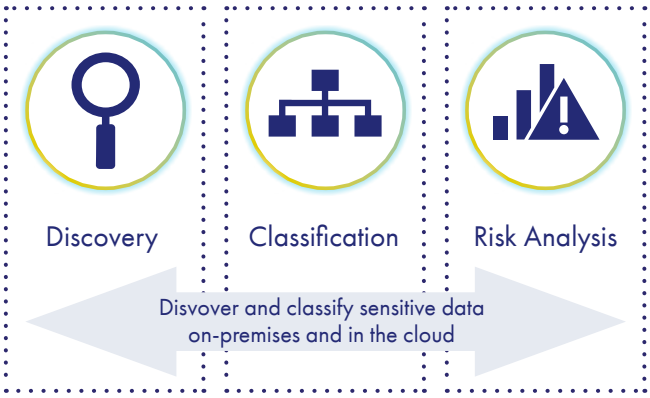
CipherTrust Platform unifies data discovery, classification, and protection and provides unprecedented granular access controls, all with centralized key management. You can rely on Thales CipherTrust Data Security Platform to discover, protect and control your organization's sensitive data, wherever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

Discover: Data Discovery & 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. It is also important to monitor and assess data regularly to ensure new data is not overlooked and your organization does not fall out of compliance.

- **CipherTrust Data Discovery and Classification** efficiently identifies structured as well as unstructured sensitive data on-premises and in the cloud. Supporting both agentless and agent-based deployment models, the solution provides built-in templates that enable rapid identification of regulated data, highlight security risks, and help you uncover compliance gaps. A streamlined workflow exposes security blind spots and reduces remediation time. Detailed reporting supports compliance programs and facilitates executive communication.

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

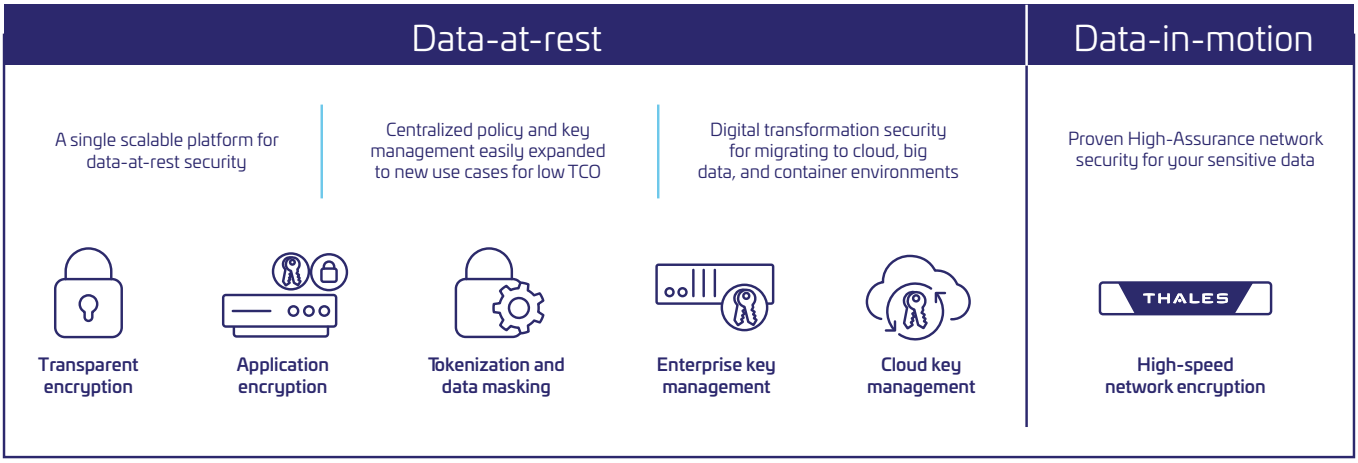


Protect Data-at-Rest

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 PDPD 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.

Data Protection

Thales Data Discovery and Classification, Protection of Sensitive Data at Rest

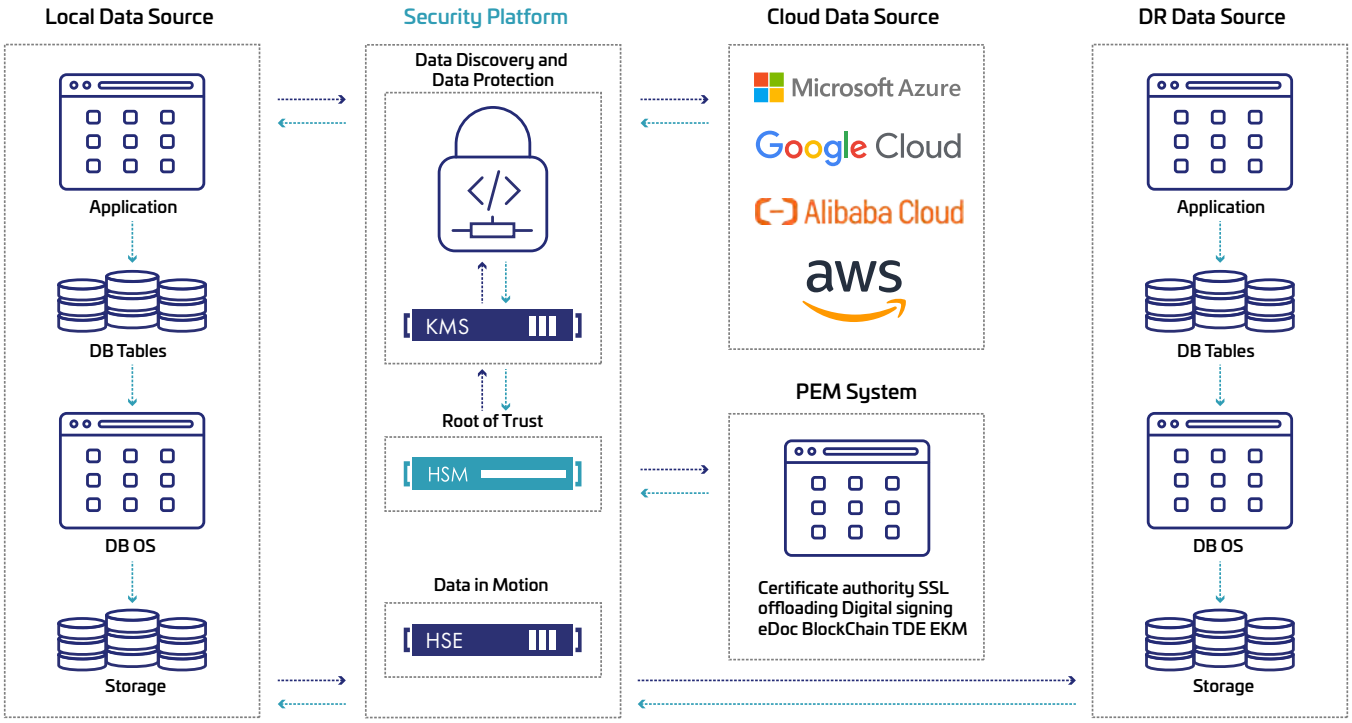


Image above: The Thales Cloud Protection & Licensing solutions in the above images consist of the following components:

√ 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!

Thales Cloud Protection & Licensing

Data Protection

Access Management & Authentication

Software Monetization

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.

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

> cpl.thalesgroup.com <

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