Compliance Brief

THALES

CYBERSECURITY

Addressing the Personal Data Protection Law in Vietnam

cpl.thalesgroup.com

THALES

CYBERSECURITY

Vietnam's Personal Data Protection Law 2025 (PDPL), enacted as Law No. 91/2025/QH15 on June 26, 2025, and effective from January 1, 2026, represents an upgrade from Decree 13/2023/ND-CP, establishing a comprehensive legal framework for the collection, use, disclosure, storage, transfer, and protection of personal data in Vietnam. The PDPL applies broadly to Vietnamese organizations, Vietnam-based entities, and foreign organizations processing personal data connected to Vietnam, while imposing clear obligations around consent, lawful processing, data subject rights, breach handling, cross-border transfers, and protective measures for high-risk data and activities.

Purpose

The core purposes of PDPL are as follows:

- Protect individual privacy and interests with clear rules on data collection, processing, storage, sharing, and transfer.
- Limit data use to specific, lawful purposes with consent or legal basis.
- Prevent misuse like unauthorized disclosure, sale, loss, or harmful processing.
- Boost accountability via duties, impact assessments, breach notices, and enforcement.
- Balance data protection with Vietnam's digital, economic, and security goals.

Scope

The PDPL applies broadly to all personal data processing activities within Vietnam, covering the following:

- Vietnamese agencies, organizations, and individuals.
- Foreign agencies, organizations, and individuals in Vietnam.
- Foreign agencies, organizations, and individuals directly engaged in or related to personal data processing of Vietnamese citizens and certain persons of Vietnamese origin residing in Vietnam.

Penalties

Article 8 of the PDPL introduces a tiered framework for maximum administrative penalties on personal data violations.

Key Penalty Highlights

- **Illegal data trading:** Up to 10x gains or VND 3 billion.
- **Cross-border transfer violations:** Up to 5% revenue or VND 3 billion.
- **Other violations:** Max VND 3 billion fine; half for individuals.
- **Enforcement:** Administrative sanctions, plus criminal penalties if severe.

How Thales Helps with the Vietnam Personal Data Protection Law 2025 (PDPL)

Thales' solutions enable organisations in Vietnam to comply with **PDPL**, particularly Chapters I, II, and III, by enhancing governance over data protection with comprehensive visibility, control, and automation. Building on the PDPL's foundational requirements, **Decree No. 356/2025/ND-CP** – released on December 31, 2025 – provides further details on personal data classification and cross-border data transfer. Thales supports organisations in aligning with both the PDPL and Decree 356, helping streamline compliance processes and ensure adherence to Vietnam's evolving regulatory framework for data protection. These capabilities also support organisations in meeting the security and data governance expectations introduced by Vietnam's Law on Artificial Intelligence (No. 134/2025/QH15), by protecting sensitive data used in AI systems through strong encryption, access controls, and data activity monitoring.

PDPL Article	How Thales Helps	Solution Areas
Chapter I – GENERAL PROVISIONS		
Article 4. Rights and obligations of data subjects **4.4:** Agencies, organizations, and individuals shall be responsible for facilitating, and shall not obstruct or hinder, the **exercise of rights and obligations** of data subjects as prescribed by law. **4.5:** Upon receipt of a request from a data subject to exercise the rights specified in Clause 1 of this Article, the personal data controller or personal data controlling and processing party shall promptly **comply within the time limit** prescribed by law.	• Identify **structured and unstructured** sensitive data at risk on premises and in the cloud. • Discover all your data and categorize it based on sensitivity and value, allowing you to **uncover hidden data** risks. • Identify the current state of compliance, document gaps, and **provide a path to full compliance**. • Gain full **sensitive data activity visibility**, track who has access, audit what they are doing and document.	**Data Security** Data Activity Monitoring Discovery & Classification
Chapter II – PERSONAL DATA PROTECTION, Section 1		
Article 10. Request for **withdrawal of consent** and request for restriction of personal data processing	• Uncover **hidden risks** with data discovery, classification, and vulnerability assessments. • **Pseudonymize sensitive** information in databases. • Gain full **sensitive data activity visibility**, track who has access, audit what they are doing and document. • Enforce **user consent** and empower customers to manage and configure their preferences.	**Data Security** Data Activity Monitoring Discovery & Classification Tokenization **Identity & Access Management** Customer Identity and Access Management
Article 12. Encryption and decryption of personal data 1. "...**Encryption of personal data** means the transformation of personal data into a form that cannot be identified..." 2. "**Personal data** classified as state secrets must be **encrypted** and decrypted in accordance with ... the law on cryptography. 3. "...Agencies, organizations... shall decide on the **encryption and decryption** of personal data in conformity with the personal data processing activities..."	• **Encrypt data** at rest on-premises, across clouds, and in big data or container environments. • Pseudonymize sensitive information in databases. • Gain **full sensitive data activity visibility**, track who has access, audit what they are doing and document. • Protect the **root-of-trust** of a cryptographic system within a highly secure environment. • Limit the access of internal and external users to systems and data based on **roles and context with policies**. • Apply **contextual security** measures based on risk scoring.	**Data Security** Data Activity Monitoring Data Discovery & Classification Data Risk Analytics Hardware Security Modules Transparent Encryption Tokenization

PDPL Article	How Thales Helps	Solution Areas
Article 14. Deletion, destruction, and de-identification of personal data **14.3:** The personal data controller or the personal data controlling and processing party shall **delete or destroy personal data** in the cases specified in Clause 1 of this Article, or shall request the personal data processor or a third party to delete or destroy the data subject's personal data. The **deletion or destruction** of personal data must be carried out using **secure measures to prevent unauthorized access** and restoration of the deleted or destroyed personal data. **14.6:** De-identification of personal data shall be conducted as follows: "... a) Agencies, organizations, and individuals that **de-identify personal data** shall be responsible for strictly controlling and supervising the de-identification process; and shall prevent unauthorized access, copying, appropriation, disclosure, or loss of personal data during the de-identification process..."	• Pinpoint sensitive data and ensure the **proper user access rights** are in place. • Employ **data activity monitoring** for structured and unstructured data across cloud and on-premises systems. • **Pseudonymize sensitive data** once it is created and make sure cleartext data will not be processed or stored by unauthorized and to prevent exposure of real data applications and personnel. • Protect sensitive data with **real-time alerting or user access blocking** of policy violations. • Remove keys from CipherTrust Manager can **ensure secure deletion**, digitally shredding all instances of the data. • Enable **Multi-factor Authentication (MFA)** with the broadest range of hardware and software methods and form factors. • Build and deploy **adaptive authentication** policies based on the sensitivity of the data.	**Data Security** Data Activity Monitoring Discovery & Classification Key Management Tokenization Transparent Encryption **Identity & Access Management** Multi-Factor Authentication Risk-Based Authentication Workforce Access Management
Article 16. Disclosure of personal data **16.1:** Personal data may only be disclosed for a specific purpose. The scope of disclosure and types of personal data to be disclosed must be consistent with the intended purpose. The disclosure of **personal data must not infringe** upon the lawful rights and interests of the data subject. **16.5:** Agencies, organizations, and individuals disclosing personal data must **closely monitor and control the disclosure** of personal data to ensure compliance with the purpose, scope, and legal regulations; and must **prevent unauthorized access**, use, disclosure, copying, modification, deletion, destruction, or other unlawful processing of disclosed personal data, within their capabilities and conditions.	• Provide **data activity monitoring** for structured and unstructured data across cloud and on-prem systems. • Identify **abnormal user behavior** and provide a complete threat description with actionable intelligence for remediation. • Support **fine-grained authorization** decisions on who may access specific resources and what actions they may perform.	**Data Security** Data Activity Monitoring Data Risk Analytics **Identity & Access Management** Externalized Authorization

PDPL Article	How Thales Helps	Solution Areas
Article 17. Transfer of personal data **Article 20.** Cross-border transfer of personal data **20.2:** Agencies, organizations, or individuals conducting cross-border personal data transfer activities as specified in Clause 1 of this Article must prepare a dossier on the **impact assessment of the cross-border transfer** of personal data and submit one original copy to the agency in charge of personal data protection within 60 days from the first day of cross-border personal data transfer, except for the cases specified in Clause 6 of this Article.	• **Encrypt data** at rest on-premises, across clouds, and in big data or container environments. • **Pseudonymize sensitive** information in databases. • Alert or block **database attacks** and abnormal access requests in real time. • **Monitor file activity** overtime to set up alerts on activity that can put the organization at risk. • Reduce **third-party risk** by maintaining on-premises control over encryption keys. • Ensure complete **separation of roles** between third party and your organization, restrict access to sensitive data. • Enable **relationship management** with suppliers, partners or any third-party user; with clear delegation of access rights. • Protect the **root-of-trust of a cryptographic** system within a highly secure environment. • Streamline reporting and analysis of user access rights to sensitive data. • Enable **multi-factor authentication (MFA)** with the broadest range of hardware and software methods. • Build and deploy **adaptive authentication policies** based on the sensitivity of the data/ application. • **Protect against phishing** and man-in-the-middle attacks. • Secure **data in transit** at Layers 2, 3, and/or 4 without slowing down the network. • Offer stronger identity and access **governance for third-party**, supplier, or cross-organization access scenarios related to transferred data. • Support **conditional access** for higher-risk or external access journeys.	**Data Security** Data Activity Monitoring Data Discovery & Classification Data Risk Analytics Hardware Security Modules High Speed Encryption Transparent Encryption User Rights Management **Identity & Access Management** Adaptive Access Control Federated Identity Management Multi-Factor Authentication Risk-Based Authentication PKI and FIDO Authenticators
Article 18. Other activities in personal data processing **18.2:** The **storage, access, retrieval, connection, coordination, confirmation, authentication of personal data**, and other operations that affect personal data shall comply with this Law, data laws, other relevant laws, and the agreement between the parties.	• Locate **structured and unstructured regulated data** across hybrid IT. • **Pseudonymize sensitive** information in databases. • **Encrypt data** at rest on-premises, across clouds, and in big data or container environments. • Manage and **monitor access controls** to enterprise-wide systems effectively. • **Log all user access** and authentication activities. • Provide **centralized user** authentication before access to applications that process personal data. • Support **federated authentication**, where applications trust a central identity provider for user authentication. • Adjust access controls based on user behavior, device, and **contextual risk** at the time of access.	**Data Security** Discovery & Classification Tokenization Transparent Encryption **Identity & Access Management** Adaptive Access Control Federated Identity Management Multi-Factor Authentication Risk-Based Authentication SafeNet Trusted Access (STA) Single Sign-On (SSO)

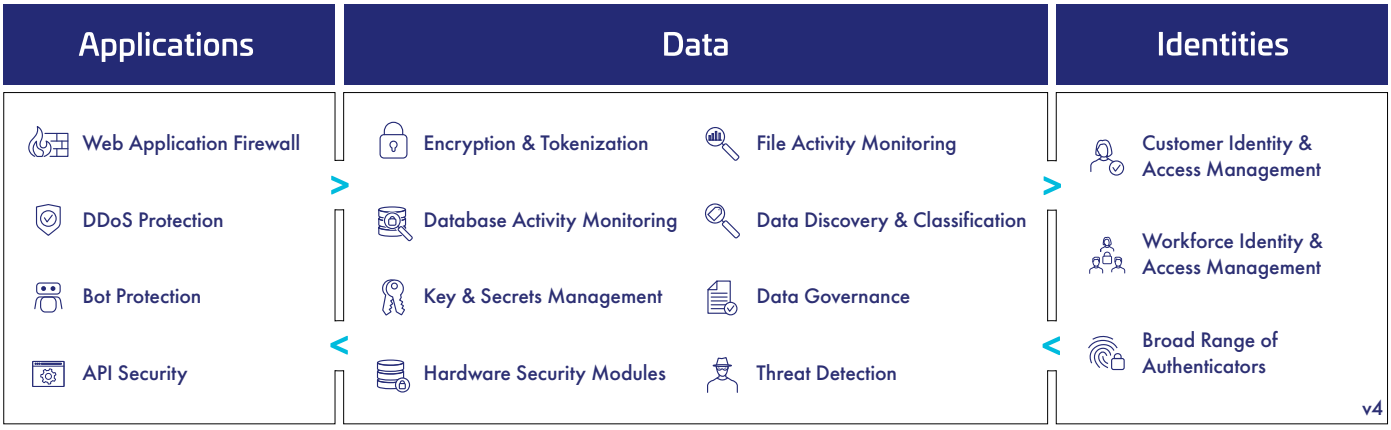
PDPL Article	How Thales Helps	Solution Areas
Article 19. Processing of personal data without requiring consent of data subjects **2b:** Implementing appropriate **personal data protection measures**; regularly assessing risks that may arise during personal data processing; **2c:** Conducting **periodic inspections and evaluations** of compliance with laws, procedures, and regulations on personal data processing;	• Provide **ongoing monitoring** of database traffic, monitoring who the users are accessing them, and provide timely alerts. • Protect personal data from **unauthorized access**, monitor what has been changed and who is accessing. • **Record access** to the database system and detect login attempts on the database system. • P**roduce audit trail and reports** of all access events to all systems, stream logs to external SIEM systems. • Manage authentication and access control by supporting **Multi-Factor Authentication** and Single Sign-On **(SSO)** and displaying access log reports. • Detect and alert administrators if **abnormal access attempts** are found, and administrators can respond quickly. • Detect and pinpoint **critical threats to data**, prioritizes what matters most, and provides actionable insights. • Support the **creation of audit trail reports** of all accesses for auditing and investigation in the event of any incidents. • Flag **access anomalies** for investigation by the security team, and integrate seamlessly with SIEM solutions for a more comprehensive approach to threat and anomaly detection. • Dynamically **evaluate the risk** level of each access attempt and apply stronger controls where the risk is higher. • Enforce **multi-factor authentication** to reduce the risk of unauthorized access across enterprise applications. • **Centralize authentication** and policy enforcement for cloud access scenarios, helping organizations apply consistent access controls.	**Data Security** Data Activity Monitoring Data Risk Analytics Transparent Encryption **Identity & Access Management** Adaptive Access Control Multi-Factor Authentication Risk-Based Authentication SafeNet Trusted Access (STA) Single Sign-On (SSO)
Article 23. Notification of violations of regulations on personal data protection **23.1**:"... In case the personal data processor detects the violation, it must **promptly notify the personal data controller** or the personal data controlling and processing party..."	• Protect data with **real-time alerting** or user access blocking of policy violations. • Identify abnormal user behavior and provide a complete threat description with **actionable intelligence** for remediation.	**Data Security** Data Activity Monitoring Data Risk Analytics

PDPL Article	How Thales Helps	Solution Areas
Chapter II – PERSONAL DATA PROTECTION, Section 2		
Article 25. Protection of personal data in the recruitment, management, and use of employees **25.2:** Responsibilities of agencies, organizations, and individuals in protecting personal data during **employee management** and use are as follows: c) Employee personal data must be **deleted or destroyed** upon termination of the employment contract, unless otherwise agreed or prescribed by law.	• **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. • **Encrypt sensitive data** once it is created and make sure cleartext data will not be processed or stored by unauthorized applications and personnel in removable media. • Provide **data activity monitoring** for structured and unstructured data across cloud and on-prem systems.	**Data Security** Data Activity Monitoring Discovery & Classification Tokenization Transparent Encryption
Article 26. Protection of personal data related to **health information and insurance business** activities **Article 27.** Protection of personal data in **financial, banking, and credit information** activities **Article 28.** Protection of personal data in **advertising service** business **Article 30.** Protection of personal data in **big data, artificial intelligence, blockchain, virtual universe, and cloud computing** **30.3:** Systems and services utilizing big data, artificial intelligence, blockchain, virtual universe, and cloud computing must integrate appropriate personal data protection measures; use suitable **authentication and identification** methods; and implement **access authorization mechanisms** for personal data processing. **Article 31.** Protection of personal data related to personal **location** data and **biometric** data **31.4:** The protection of biometric data is prescribed as follows: a) Agencies, organizations, and individuals collecting and processing biometric data must **implement physical security measures for their biometric data storage and transmission devices**; restrict access to biometric data; **establish monitoring systems to prevent and detect** acts of infringement of biometric data; and comply with the law and relevant international standards;	• **Discover all of your data** and categorize it based on sensitivity and value, allowing you to uncover hidden data risks. • Deliver **data-at-rest encryption** with centralized key management, privileged user access control and detailed data access audit logging. • Apply **privileged access control** to sensitive data. • **Pseudonymize** sensitive information in databases. • Gain visibility by **monitoring and auditing all database** activity. • Detect and pinpoint **critical threats to data**, prioritizes what matters most, and provides actionable insights. • **Protect the root-of-trust** of a cryptographic system within FIPS 140-2 Level 3 - a highly secure environment. • Leverage **smart cards** for implementing physical access to sensitive facilities. • **Record access** to the database system and detect login attempts on the database system. • Manage authentication and access control by supporting **Multi-Factor Authentication** and Single Sign-On (SSO) and displaying access log reports. • **Produce audit trails and reports** of all access events to all systems, **stream logs** to external SIEM systems. • Detect and alert administrators if **abnormal access attempts** are found, and administrators can respond quickly. • Flag **access anomalies** for investigation by the security team, and integrate seamlessly with SIEM solutions for a more comprehensive approach to threat and anomaly detection. • Offer **multiple authentication** methods suitable for different access scenarios and data sensitivity levels. • Support **passwordless access** journeys that reduce dependency on passwords in modern digital environments.	**Data Security** Data Activity Monitoring Data Risk Analytics Discovery & Classification File Activity Monitoring Hardware Security Modules Key Management Transparent Encryption **Identity & Access Management** Adaptive Access Control FIDO Passkeys and Devices Multi-Factor Authentication On Premises Authentication Management Passwordless Authentication PKI USB Tokens Risk-Based Authentication Workforce Access Management SafeNet Trusted Access (STA) Single Sign-On (SSO)

PDPL Article	How Thales Helps	Solution Areas
	• Employ **certificate-based** strong authentication for higher-assurance access scenarios. • Provide **on-premises** authentication management for enterprise environments that require internal control over authentication infrastructure. - • Enforce **strong user authentication** before access to systems that handle biometric or other sensitive personal data. • Apply **contextual access policies** to restrict who can reach sensitive systems and under what conditions. • Enable stronger identity assurance using **device-bound** modern authenticators suitable for sensitive access journeys. • Provide **centralized access** and authentication controls for sensitive applications.	
Article 32. Protection of personal data collected from **audio and video recording** activities in public places and public activities **5.** Agencies, organizations, and individuals conducting audio and video recording and processing personal data collected from such recordings in the cases specified in Clause 1 of this Article shall be responsible for **protecting personal data** in accordance with this Law and other relevant laws.	• **Encrypt sensitive data** once it is created and make sure cleartext data will not be processed or stored by unauthorized applications and personnel in removable media. • **Protect sensitive personal data** whether it is in applications or databases and replace sensitive values with format-preserving tokens. • Provide **ongoing monitoring** of database traffic, monitoring who the users are accessing them, and provide timely alerts. • Protect personal data from **unauthorized access**, monitor what has been changed and who is accessing.	**Data Security** File Activity Monitoring Tokenization Transparent Encryption
Chapter III – FORCES, CONDITIONS FOR PROTECTION OF PERSONAL DATA		
Article 37. Responsibilities of personal data controllers, personal data processors or personal data controlling and processing parties **2. Responsibilities of personal data processors:** c) To fully perform personal data protection measures in accordance with this Law and other relevant laws.	• Provide **ongoing monitoring** of database traffic, monitoring who the users are accessing them, and provide timely alerts. • Protect personal data from **unauthorized access**, monitor what has been changed and who is accessing. • **Detect anomaly** behavior and provide deeper insight.	**Data Security** Data Activity Monitoring

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

Security for What Matters Most



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.

Disclaimer: The information contained herein is believed to be accurate on the date of publishing. Thales provides this material for your information only. Its content is not legal advice nor does it amount to a certification or guarantee of compliance in respect of any applicable law. Third parties shall be solely responsible for their own interpretation of any applicable law. The information should not be construed as a commitment to deliver any specific upgrade, feature or functionality. You should not rely on the anticipated timelines or potential upgrades, features or functionality described in the presentation when making a decision to purchase products from Thales. Thales does not accept any liability howsoever arising from any use of this material.

© Thales - May 2026 • EHv5