Compliance Brief

THALES
CYBERSECURITY

Addressing the requirements of NPC Circular 2023-06 for the Security of Personal Data in the Philippines

cpl.thalesgroup.com

THALES

CYBERSECURITY

Introduction

The National Privacy Commission (NPC) introduces circulars to provide organizations with guidance on complying with the Data Privacy Act of 2012 in the Philippines, its implementing rules and regulations, and other NPC issuances. On April 1, 2024, the NPC issued Circular 2023-06 to strengthen personal data protection in the Philippines by governing the security of personal data in the government and private sector.

The Philippines Data Privacy Act protects personal information. The National Privacy Commission (NPC) was established as the lead agency to implement the law and ensure the country's compliance with international standards of data protection.

NPC Circular 2023-06

The NPC Circular 2023-06 for the Security of Personal Data in the Government and Private Sector provides updated requirements for the security of personal data processed by a personal information controller (PIC) or a personal information processor (PIP). The Circular also sets provisions on the storage of personal data, ensuring data subjects' information is stored for the necessary duration and protected through industry standards and best practices.

Additionally, the Circular outlines stringent provisions for access to personal data, specifying procedures for authorized personnel, acceptable use policies, secure authentication mechanisms, and measures for remote disconnection or deletion of data on mobile devices, among others.

Penalties

Violating the Circular may result in the issuance by the NPC of compliance and enforcement orders, cease and desist orders, temporary or permanent ban on the processing of personal data, or payment of fines against the PIC or PIP. In addition, failure to comply with the Circular may result in criminal, civil and administrative liabilities and disciplinary sanctions against any erring officer or employee of the PIC or PIP.

There is a transitory period of 12 months from the effectivity of the Circular or until 30 March 2025 to comply with the foregoing requirements.

How can Thales help with the NPC Circular 2023-06

Thales helps organizations comply with Circular 2023-06 by addressing some of the sections on Privacy Impact Assessment (PIA), Control Framework for Data Protection, Privacy-By-Design and Privacy-By-Default, Storage, Access and Disposal of Personal Data.

NPC Circular 2023-06	Thales Solutions
SECTION 5. Privacy Impact Assessment (PIA) - a data inventory "A PIA should be undertaken for every processing system of a PIC or PIP that involves personal data..."	A crucial step is understanding what constitutes sensitive data, where and how it is stored, and who can access it, and introducing data activity monitoring. • **CipherTrust Data Discovery & Classification** discovers and classifies data in all the data stores in an organization's data estate, from structured to semi-structured to unstructured across on-premises, hybrid, cloud, and multi-cloud environments. This visibility enables organizations to build a robust data privacy and security foundation. • **Imperva Data Security Fabric Data Activity Monitoring (DAM)** not only continuously discovers and classifies valuable data; structured, semi-structured, and unstructured, it also provides proactive controls and predictive analytics for activity monitoring, security assessments, risk modeling, and attack detection. DSF allows you to standardize your data security controls for complete visibility and centralized command across all your file stores and data assets, on-premises, in the hybrid cloud, and across multiple clouds. DSF's flexible architecture supports a broad range of data repositories, from legacy mainframe systems to modern data lakes and everything in between, whether the data is structured or unstructured. ◦ **Imperva Data Security Fabric (DSF)** enhances data governance by discovering and mapping file and database servers and identifying sensitive data such as social security numbers, credit card data, etc. It allows organizations to understand current data usage, enabling role and workflow management of data to grant access to data stewards and create reports around data for compliance reporting. ◦ **Imperva Data Security Fabric Data Risk Analytics (DRA)** monitors and analyzes all data access and activity by both database user accounts and privileged user accounts and can automatically determine if a data access event violates a compliance or security policy. It delivers real-time alerting and user access blocking of policy violations and cost-effectively retains years of data for audits. Combining deep domain security expertise with machine learning (ML) allows organizations to identify suspicious user and computer system behaviors that violate security policies, practices, and peer group norms.
SECTION 6. Control Framework for Data Protection "The risks identified in the PIA must be addressed by a Control Framework..."	Continuous monitoring captures and analyzes all data store activity, in the cloud or on-premises, 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.
RULE II: EMBEDDING PRIVACY-BY-DESIGN AND PRIVACY-BY-DEFAULT	
SECTION 7. Privacy-By-Design and Privacy-By-Default	Organizations can secure sensitive data privacy by design with Thales Tokenization and Transparent Encryption. • **CipherTrust Tokenization** permits the pseudonymization of sensitive information in databases while maintaining the ability to analyze aggregate data without exposing sensitive data during the analysis or in reports. • **CipherTrust Transparent Encryption** encrypts sensitive data and enforces granular privileged-user-access management policies that can be applied by user, process, file type, time of day, and other parameters. It provides a complete separation of roles, where only authorized users and processes can view unencrypted data. Organizations can add an additional layer of protection with a second identity verification step at the access point with Multi-Factor Authentication (MFA) with CipherTrust Transparent Encryption. This can limit privileged users' accessing sensitive data.

NPC Circular 2023-06	Thales Solutions
RULE III. STORAGE OF PERSONAL DATA	
SECTION 10. Service Provider as Personal Information Processor **SECTION 11. Protection of Personal Data.** "All personal data that are processed must be adequately protected through industry standards and best practices..."	Encryption plays a vital role in storing data and protecting data's confidentiality, integrity, and availability across its lifecycle. Depending on your security requirements and infrastructure, different approaches can be used to protect data-at-rest in files, volumes, and databases. CipherTrust Data Security Platform provides multiple capabilities for protecting data at rest in files, volumes, and databases. **Transparent Encryption** operates at the file system layer, delivering data-at-rest encryption with centralized key management, granular access controls, and data access logging to meet best practice requirements for protecting data. To protect data-at-rest from zero-day and privileged escalation attacks, **ransomware protection** uses real-time behavior monitoring to alert or block malicious activity before ransomware can take hold of data. Database protection at the database layer supports key management for native TDE use cases or the ability to do field or column-level encryption on databases. At the **application layer**, libraries for C and Java can be deployed, or solutions at the network layer can be used as a gateway to apply encryption without modifying the application code. Organizations can enhance protection of sensitive data by masking them with **CipherTrust Data Security Platform** through below: • 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 Transparent Encryption encrypts sensitive data and enforces granular privileged-user-access management policies that can be applied by user, process, file type, time of day, and other parameters. It provides complete separation of roles where only authorized users and processes can view unencrypted data. Unless a valid reason to access the data is provided, sensitive data stored in a third-party cloud will not be accessible in cleartext to unauthorized users. These could include third-party cloud provider employees, such as support engineers, DB admins, or potentially malicious processes. • CipherTrust Enterprise Key Management streamlines and strengthens key management in cloud and enterprise environments over a diverse set of use cases, encrypted information can be effectively deleted by destroying encryption keys. Leveraging FIPS 140-2-compliant virtual or hardware appliances, Thales key management tools and solutions deliver high security to sensitive environments and centralize key management for home-grown encryption, as well as third-party applications.

NPC Circular 2023-06	Thales Solutions
RULE IV. ACCESS TO PERSONAL DATA	
SECTION 12. Access to or Modification of Databases. **SECTION 13. Restricted Access** **SECTION 16. Online Access to Personal Data** "implement secure authentication mechanisms, such as multifactor authentication or secure encrypted links..."	**Imperva Data Security Fabric Data Risk Analytics** monitors data access and activity for all databases. It provides the visibility needed to pinpoint risky data access activity for all users, including privileged users. Organizations can uncover hidden risks and vulnerabilities while creating reports to effectively communicate risk and ongoing activities. It delivers real-time alerting and user access blocking of policy violations and cost-effectively retains years of data for audits. Combining deep domain security expertise with machine learning (ML) allows organizations to identify suspicious user and computer system behaviors that violate security policies, practices, and peer group norms. **CipherTrust Transparent Encryption (CTE)** helps organizations control access to restricted information by encrypting sensitive data and enforcing granular privileged-user-access management policies that user, process, file type, time of day, and other parameters can apply. CTE provides a complete separation of roles where only authorized users and processes can view unencrypted data with detailed data access audit logs. This protects data wherever it resides, on-premises, across multiple clouds, and within big data and container environments. **Thales Identity and Access Management Solutions** limit the access of internal and external users based on their roles and context. Backed by strong authentication (MFA), granular access policies and fine-grained authorization policies help ensure the right user is granted access to the right resource at the right time. This minimizes the risk of unauthorized access. **Thales SafeNet Trusted** Access is a cloud-based access management solution that makes it easy to manage access to both cloud services and enterprise applications with an integrated platform combining single sign-on, multi-factor authentication (MFA) and scenario-based access policies. It provides a single pane view of access events across your app estate to ensure that the right user has access to the right application at the right level of trust. STA also offers an up-to-date audit trail of all access events to all systems. Extensive automated reports document all aspects of access enforcement and authentication.
RULE VII. GUIDELINES FOR DISPOSAL OF PERSONAL DATA	
SECTION 28. Disposal and Destruction of Personal Data **SECTION 29. Logs Retention** **SECTION 30. Procedures for Disposal and Destruction.** "Electronically disposing or destroying personal data in storage media which involve the use of degaussers, erasers, encryption, or secure wiping program..." **SECTION 31. Personal Data Disposal Service Provider.** "engage a PIP to carry out the disposal of personal data under its control..."	**CipherTrust Transparent Encryption (CTE)** and **CipherTrust Tokenization** offer a "crypto-shreds" function that destroys the encryption key for the encrypted data and ensures that the information cannot be restored. **CipherTrust Enterprise Key Management** ensures secure asset disposal; it streamlines and strengthens key management in cloud and enterprise environments over a diverse set of use cases; encrypted information can be effectively deleted by destroying encryption keys. Leveraging FIPS 140-2-compliant virtual or hardware appliances, Thales key management tools and solutions deliver high security to sensitive environments and centralize key management for home-grown encryption, as well as third-party applications.

NPC Circular 2023-06	Thales Solutions
RULE VIII. MISCELLANEOUS PROVISIONS	
SECTION 32. Threat monitoring and vulnerability management.	Threat monitoring is one crucial capability for organizations to prevent, detect, and respond to a cyberattack. Imperva Data Security Fabric and Thales CipherTrust Transparent Encryption Ransomware Protection can help organizations address this challenge. • **Imperva Data Security Fabric Data Risk Analytics** monitors data access and activity for all databases and provides the visibility needed to pinpoint risky data access activity for all users, including privileged users. - Organizations can uncover hidden risks and vulnerabilities while creating reports to effectively communicate risk and ongoing activities. - It delivers real-time alerting and user access blocking of policy violations and cost-effectively retains years of data for audits. - Combining deep domain security expertise with machine learning (ML) allows organizations to identify suspicious user and computer system behaviors that violate security policies, practices, and peer group norms. Purpose-built detection algorithms instantly recognize active attack exploits and immediately send incident alerts. • **CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP)** continuously monitors processes for abnormal I/O activity and alerts or blocks malicious activity before ransomware can take complete hold of your endpoints and servers. It monitors 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.

Visibility and Control: Thales and Imperva

Thales and Imperva, a Thales company, deliver a broad portfolio of complementary application security, data security, and identity & access management products to provide comprehensive solutions that help address NIS2 requirements. The portfolio delivers comprehensive data-centric security that protects data and all paths to it with platforms that reduce the complexity and risks of managing applications, data, and identities in the cloud.

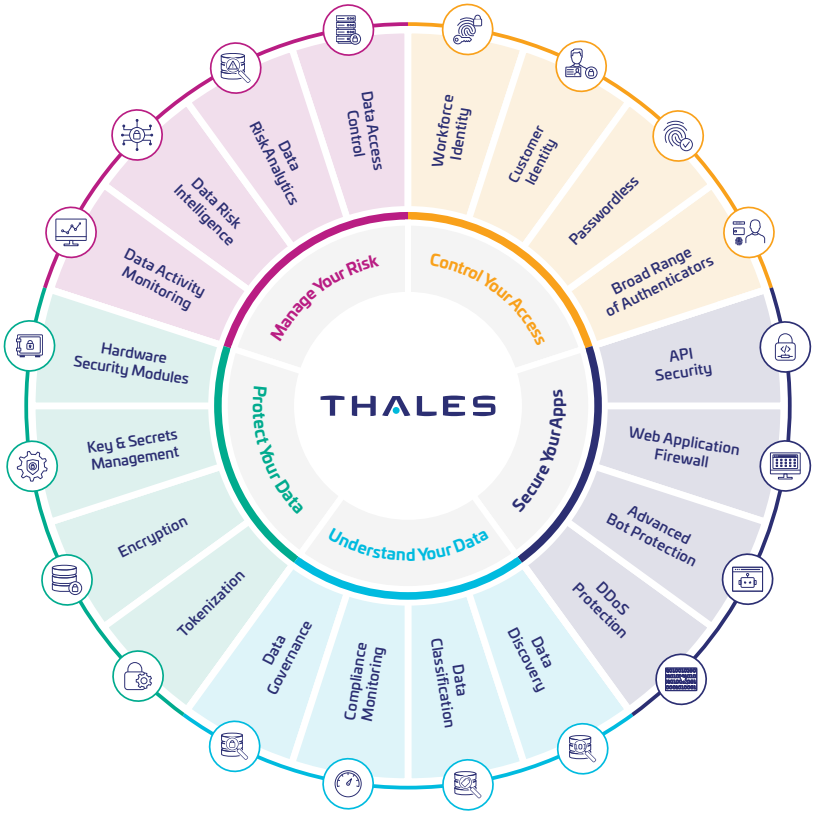
Organizations can leverage Thales' suite of identity and data security solutions available on a single unified platform to become compliant today and stay compliant in the future. Contact us now!

Security for What Matters Most

Applications	Data		Identities
Web Application Firewall	Encryption	File and Data Activity Monitoring	Customer Identity & Access Management
DDoS Protection	Tokenization	Data Discovery & Classification	Workforce Identity & Access Management
Bot Protection	Key & Secrets Management	Data Governance	Broad Range of Authenticators
API Security	Hardware Security Modules	Threat Detection	

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.



cpl.thalesgroup.com

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us

© Thales - January 2026 • EHv5