thalesesecurity.com

THALES

Data security best practices for complying with the Philippines Data Privacy Act

White Paper

Executive Summary

If your organization manages the personal data of Philippine citizens or has information services running in the Philippines, complying with the Data Privacy Act is now a vital imperative. This white paper offers an overview of the Data Privacy Act, and then it provides an in-depth look at how the Vormetric Data Security Platform from Thales eSecurity can deliver the robust capabilities that help address many of the act's data-at-rest security requirements.

Introduction to the Data Privacy Act

In 2012, the Philippines government enacted a comprehensive data privacy law. The Data Privacy Act of 2012 was established to protect individuals' fundamental rights to privacy, while enabling the free flow of information that is required to promote innovation and growth.

As part of the act, the formation of a National Privacy Commission was initiated. The National Privacy Commission's charter was to institute rules and regulations as well as monitor and enforce compliance. While the Data Privacy Act was implemented in 2012, the National Privacy Commission wasn't officially established until 2016, and it was only in September of that year that the commission's rules and regulations were finalized and put into effect.

The Data Privacy Act is broadly applicable to individuals and legal entities that process personal information. The law applies to the processing of the personal information of Philippines citizens, regardless of where the business may reside. The law applies not only to businesses with offices in the Philippines, but those that use equipment based in the Philippines for processing.

The law defines sensitive personal information as including the following:

- Demographic information, including race, marital status, education, age and religious and political affiliations.
- Health and genetic information.
- Legal information, including any offenses or alleged offenses.
- Specific government-issued information that is unique to an individual, such as social security numbers.

The law prohibits the sharing of any of this personal information, except in certain circumstances, such as when legally approved or mandated, specifically approved by an individual or when required for medical emergencies.

For enterprises, it is vital to recognize that the Data Privacy Act represents another mandate that places an emphasis on the safeguarding of sensitive data—and imposes significant penalties on those that fail to comply. If an organization fails to comply with the Data Privacy Act, responsible parties may face up to six years of imprisonment and fines of up to $100,000.

The law specifies that any entity involved in the processing of personal data must establish formal security and privacy programs. Organizations must develop, implement and review policies and procedures for how this data is collected, controlled, accessed and retained. The law also requires the implementation of appropriate data protection policies that provide for organizational, physical and technical security measures. The following sections focus on how organizations can address these technical security requirements.

Effectively address data-at-rest security guidelines with the Vormetric Data Security Platform

With the Vormetric Data Security Platform, you can effectively manage data-at-rest security across your entire organization. Built on an extensible infrastructure, the Vormetric Data Security Platform delivers centralized key and policy management for a suite of data security solutions that secure your organization's sensitive and regulated data wherever it resides. As a result, your security teams can efficiently address many of the guidelines specified by the Data Privacy Act as well as your data security policies, other compliance mandates and best practices—all while reducing administration effort and total cost of ownership.

The platform offers capabilities for protecting and controlling access to databases, files and containers— and can secure assets residing in cloud, virtual, big data and physical environments. This scalable, efficient data security platform enables you to address your urgent requirements, and it prepares your organization to respond nimbly when the next security challenge or compliance requirement arises.

The Vormetric Data Security Platform features these products:

- **Vormetric Data Security Manager.** Delivers centralized controls that enable consistent and repeatable management of encryption, access policies and security intelligence for all your structured and unstructured data. Available as FIPS 140-2 and Common Criteria certified virtual and physical appliances.
- **Vormetric Transparent Encryption.** Features a software agent that runs in the file system to provide high-performance encryption and least-privileged access controls for files, directories, and volumes. Enables encryption of both structured databases and unstructured files. Vormetric Transparent Encryption offers the patented capability of Live Data Transformation, which allows users to encrypt and rekey data without downtime.
- **Vormetric Tokenization with Dynamic Data Masking.** Easy to implement format-preserving tokenization to protect sensitive fields in databases and to deliver policy-based dynamic data masking for display security.
- **Vormetric Application Encryption.** Streamlines the process of adding both NIST-standard AES encryption and format-preserving encryption (FPE) into existing applications. Offers standards-based APIs that can be used to perform high-performance cryptographic and key management operations.
- **Vormetric Key Management.** Provides unified key management to centralize management and secure storage of keys for Vormetric Data Security Platform products, TDE, and KMIP compliant clients as well as securely stores certificates.
- **CipherTrust Cloud Key Manager.** Offers capabilities for establishing strong governance over encryption keys and policies, so you can fully leverage SaaS environments while minimizing complexity and risk.

"We have examined many data encryption solutions—including native database encryption offerings—and the Vormetric Data Security Platform scored well above these other alternatives. The solution's proof of concept went smoothly, and was completed within two days."

- Executive at Philippines Bank that employed the Vormetric Data Security Platform to address Data Privacy Act requirements

- **Vormetric Protection for Teradata Database.** Makes it fast and efficient to employ robust data-at-rest security capabilities in your Teradata environments. Offers granular protection, enabling encryption of specific fields and columns in Teradata databases.
- **Vormetric Security Intelligence.** Produces granular logs that provide a detailed, auditable record of file access activities, including root user access. Offers integration with security information and event management (SIEM) systems' Vormetric dashboards and reports that streamline compliance reporting and speed threat detection.
- **Vormetric Orchestrator.** Automates deployment, configuration, management and monitoring of select Vormetric Data Security Platform products. Offers capabilities that simplify operations, help eliminate errors and speed deployments by automating repetitive tasks.
- **Vormetric Batch Data Transformation.** Makes it fast and easy to mask, tokenize or encrypt sensitive column information in databases. Can be employed before protecting existing sensitive data with Vormetric Tokenization or Vormetric Application Encryption. Delivers static data masking services.

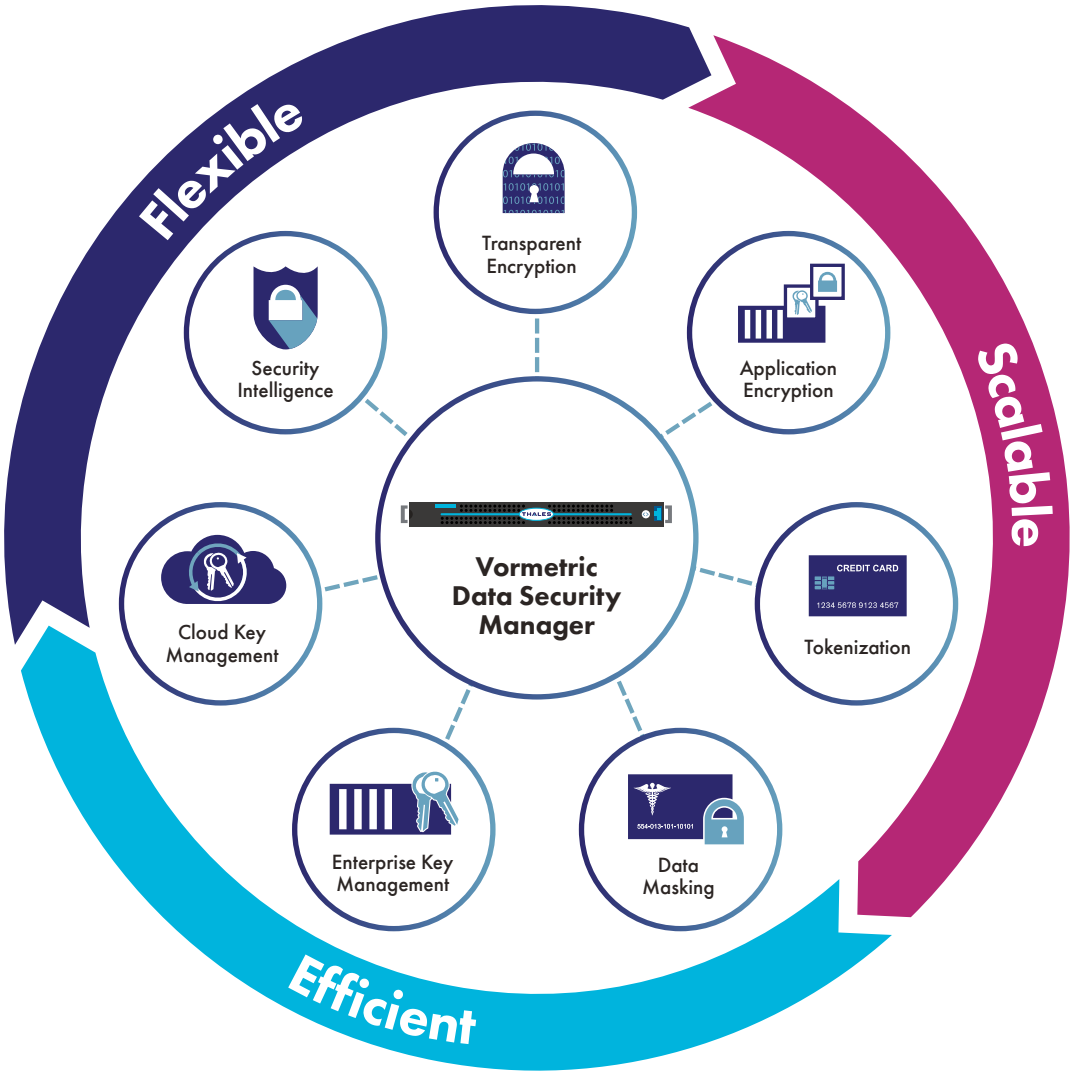

Figure 1 - The Vormetric Data Security Platform delivers extensible and efficient data security

Requirements Vormetric Data Security Platform addresses

The Vormetric Data Security Platform can help you address a number of technical security measures that are required by the Data Privacy Act. Following are a listing of many of the relevant requirements, and an overview of how the solution can help:

Requirement	How the Vormetric Data Security Platform addresses the mandate
Implement appropriate data protection policies that provide for organization, physical, and technical security measures.	The Vormetric Data Security Platform provides a centralized and secure platform for managing encryption keys and data access policies. The solution enables customers to implement enterprise data protection policies across structured and unstructured data in a range of environments, including Linux and Windows platforms.
Maintain records that sufficiently describe their data processing system and identify the duties and responsibilities of those individuals who will have access to personal data.	The Vormetric Data Security Platform offers the capabilities needed to establish strict separation of duties. With the platform, a security officer can establish strong security policies through the Vormetric Data Security Manager console. Through these controls, organizations can ensure that security administrators are able to manage cryptographic keys and data access policies, while system administrators can only handle tasks associated with database server administration. Further, policies can be enforced to ensure that one administrator does not have complete control over data security activities, encryption keys or administration.
Develop, implement and review policies and procedures for the collection and processing of personal data, for data subjects to exercise their rights under the DPA, access management, system monitoring, protocols for security incidents or technical problems, and data retention.	The Vormetric Data Security Platform provides a centralized and secure platform for managing encryption keys and data access policies. With the solution, customers can implement enterprise data protection policies across structured and unstructured data residing in a range of environments.
Adopt and establish technical security measures such as, but not limited to, security policy for the processing of personal data; safeguards to protect their computer network, periodic evaluation of security measures' effectiveness; and personal data encryption.	The Vormetric Data Security Platform delivers granular event logs that provide an auditable trail of permitted and denied access attempts to protected data. With the solution, logging occurs at the file system level and integrates with centralized SIEM systems to streamline compliance and security reporting. Through this centralized platform and its granular controls, security teams can establish strong safe-guards against abuse by privileged insiders.

Requirement	How the Vormetric Data Security Platform addresses the mandate
Section 28. Guidelines for Technical Security Measures. Where appropriate, personal information controllers and personal information processors shall adopt and establish the following technical security measures:	
a. A security policy with respect to the processing of personal data;	The Vormetric Data Security Platform enables customers to leverage data encryption and privileged user access control to safeguard confidential information, including data residing in physical, virtual, big data, container and cloud environments. The solution provides a centralized and secure platform for encryption key and policy management, which enables customers to implement enterprise data protection policies across their organizations.
b. Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;	According to Forrester and other analysts, 80% of data breaches involve the compromise of administrative credentials. The reason for this is "admin credentials" allow a user access to all data and the ability to edit logs to remove traces of their visit. Vormetric Transparent Encryption delivers privilege user access control that allows administrators to do their job without allowing these users to see the data in clear-text, hence preventing unauthorized data access. It also protects logs and reports from being tampered with.
c. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;	The Vormetric Data Security Platform enables organizations to secure confidential customer data through strong data encryption and privileged user access controls. With the solution, security teams can enforce least-privileged user access control policies to specific users, processes and resources. As a result, only assigned resource owners and security administrators can authorize and approve access to sensitive data. Vormetric Transparent Encryption features an agent-based architecture that enables encryption to be performed on servers. As a result, the solution eliminates the bottlenecks that plague legacy, proxy-based solutions, which route all information through fixed nodes on networks. The Vormetric Data Security Manager features redundant components and the ability to cluster appliances for fault tolerance and high availability. Strong separation-of-duties policies can be enforced to ensure that one administrator does not have complete control over data security activities, encryption keys or administration.
d. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach;	Vormetric Security Intelligence logs delivers detailed, actionable security event logs that provide unprecedented insight into file access activities. With the solution, your organization can leverage immediate alerts that fuel automated escalation and response. These logs are easy to integrate with SIEM systems, so you can efficiently track and investigate suspicious activities and produce compliance and security reports.

Requirement	How the Vormetric Data Security Platform addresses the mandate
e. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;	The Vormetric Data Security Platform offers a range of capabilities that help ensure the fast availability of encryption keys and encrypted data. Vormetric Key Management offers secure replication of keys across multiple appliances with automated backups. In addition, the solution can work seamlessly with your existing backup and replication solutions, including DB2 backup, NetBackup, NetWorker, NTBackup, Oracle Recovery Manager (RMAN), Windows Server and Volume Shadow Copy Service (VSS). With Live Data Transformation, security teams can encrypt data without downtime or disruption to users, applications or workflows. The solution offers advanced key versioning management capabilities, providing efficient backup and archive recovery that enables more immediate access.
f. A process for regularly testing, assessing, and evaluating the effectiveness of security measures;	Most of our enterprise customers apply encryption in testing environments before they deploy to production, and our solutions offer a range of capabilities that support these efforts. Vormetric Transparent Encryption provides "learn mode" capabilities that can help security teams understand existing application usage patterns before they apply encryption and access controls to production environments. In addition, the Vormetric Data Security Platform provides fine-grained auditing and reporting, enabling security teams to review and assess the security measures being employed on data at rest.
g. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.	The Vormetric Data Security Platform offers capabilities for establishing encryption and privileged user access controls around confidential customer data. Vormetric Transparent Encryption offers encryption and least-privileged access controls for files, directories and volumes. With the solution, security teams can ensure only authorized users and administrators can access sensitive personal data.

About Thales Cloud Protection & Licensing

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

THALES

Americas – Thales eSecurity Inc.
2860 Junction Avenue, San Jose, CA 95134 USA
Tel: +1 888 744 4976 or +1 954 888 6200
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: asia.sales@thales-esecurity.com

Europe, Middle East, Africa
Meadow View House, Long Crendon,
Aylesbury, Buckinghamshire HP18 9EQ
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalesesecurity.com <