Compliance Brief

Data Security Compliance for The Act on the Protection of Personal Information in Japan

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

The Act on the Protection of Personal Information was enacted on May 15 and fully enforced in April 2003, aiming to protect the rights and interests of individuals (APPI) while considering the usefulness of personal information. Information such as name, gender, date of birth, and address is important information related to personal privacy. Utilizing this information can improve services and operational efficiency in various fields such as government, medical care, and business.

The APPI has been revised three times to respond to changes in economic and social conditions such as the progress of digital technology and globalization, as well as the growing awareness of personal information globally, the latest revision which enforced on Apr 4, 2022, has consolidated and integrated the rules of private businesses, national administrative agencies, independent administrative agencies, and other local government agencies and local incorporated administrative agencies.

How can Thales help with compliance for The Act on Protection of Personal Information?

As the leader in digital security and data protection, Thales has helped hundreds of enterprises comply with regulations worldwide by recommending the appropriate data protection technologies required to meet regulatory requirements. Thales helps Japanese organizations comply with the Act on Protection of Personal Information (General Rule) by addressing essential requirements for advanced encryption and key management. Organizations can leverage Thales' suite of identity and data security solutions to become compliant today and stay compliant in the future.

Act on Protection of Personal Information

2-1- Personal information (related to Article 2, Paragraph 1 of the Act)

"Information about an individual" is not limited to information that identifies an individual such as name, address, gender, date of birth, facial image, etc., but also facts, judgments, and evaluations regarding attributes such as an individual's body, property, occupation, title, etc. This includes all information that represents public information such as evaluation information, public publications, etc., as well as video and audio information, regardless of whether or not it has been concealed through encryption, etc.

Reporting is not required in cases where "advanced encryption and other measures necessary to protect the rights and interests of individuals" are taken, such as when secrecy such as advanced encryption is used.

3-5-3-1 Situations to be reported

In addition, if personal data that has been or is likely to be leaked has been anonymized by advanced encryption, etc., "advanced encryption or other methods necessary to protect the rights and interests of individuals" No report is required if appropriate measures have been taken.

10-3 Organizational safety management measures

(2)**Operation in accordance with regulations regarding the handling of personal data**
Personal data must be handled in accordance with pre-established regulations for handling personal data. Furthermore, it is also important to record the usage status to confirm the status of the operation in accordance with established regulations of handling personal data.

(3)**Establishment of means to confirm the handling status of personal data**
Means must be put in place to confirm the status of handling of personal data.

(4)**Establishment of a system to respond to incidents such as leaks**
A system must be put in place to respond appropriately and promptly in the event that an incident of such are detected.

Thales Solutions

Encryption and tokenization can successfully secure sensitive data such as personal information, the cryptographic keys themselves must be secured, managed and controlled by the organization to further enhance data security.

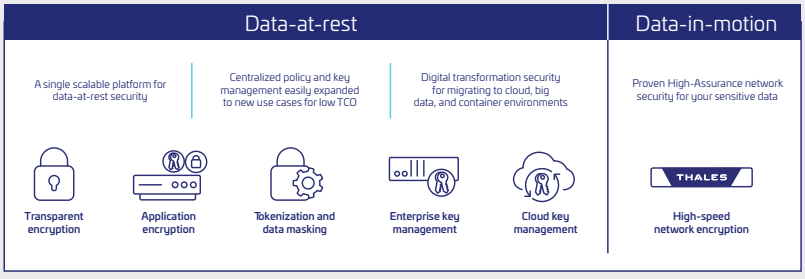
Protect sensitive data:

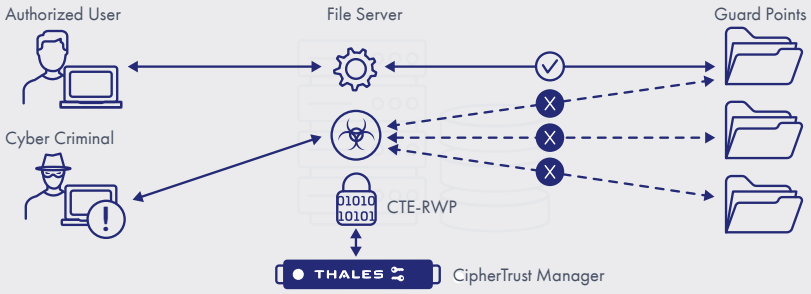
- **CipherTrust Tokenization** provides comprehensive data security capabilities, including file-level encryption with access controls, application-layer encryption, database encryption, static data masking, vaultless tokenization with policy-based dynamic data masking, and vaulted tokenization to support a wide range of data protection use cases.
- **CipherTrust Transparent Encryption (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.

Control:

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

- **CipherTrust Manager** is an Enterprise Key Management (EKM) solution that enables a single, centralized platform for managing cryptographic keys and applications.
  - centralizes encryption key management for Oracle Database and Microsoft SQL Server TDE as well as a variety of additional Thales and third-party encryption solutions
  - support Key Management Interoperability Protocol (KMIP) for key life-cycle management between encryption systems and enterprise applications, such as MySQL, MongoDB, SAN storage VMWare Infrastructure, Tape Libraries, and more
  - allow administrators to simultaneously manage multiple, disparate encryption appliances and associated keys through a single, centralized key management platform
- **CipherTrust Cloud Key Management (CCKM)** offers keys lifecycle control, centralized management within and among clouds, and visibility of cloud encryption keys. It protects your time as well as your data with a single pane of glass view across regions for cloud native, BYOK and HYOK keys and one straightforward UI to manage all cloud Key Management Services.
- **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. In addition, the CipherTrust Manager supports two-factor authentication for administrative access.



Act on Protection of Personal Information	Thales Solutions
10-6 Technical safety control measures (4) **Prevention of leaks, etc. associated with the use of information systems** Ensure safety when designing information systems and continually review them (including taking measures against attacks that exploit the vulnerabilities of information systems). Encrypt the route or content of communications, including personal data. Personal data to be transferred will be protected using passwords, etc. Set password for a file that containing personal data when sending it via email.	Network encryption can protect data in motion and ransomware protection solution helps organizations detect cyber attacks and secure sensitive data. • **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. • **CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP)** provides a non-intrusive way of protecting files/folders from ransomware attacks. It 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.  CipherTrust Transparent Encryption - Ransomware Protection (CTE-RWP)

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, identity & access management, 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.