THALES

thalescpl.com

# Thailand’s Personal Data Protection Act and What it Means for Your Business

A quick look at the changes in Thailand’s personal data protection laws in 2019. Here are the highlights of the amendments to the law along with its implications.

# What is it?

After nearly two decades in the making, Thailand's Personal Data Protection Act was approved and endorsed by the National Legislative Assembly on 28 February 2019. It was published in the Government Gazette on May 27, 2019 and will be passed into law during the latter part of 2019.

The new Act shares concepts similar with the General Data Protection Regulation (GDPR) in terms of consent, legal processing and notification, as well as definitions of data and the roles of the Data Protection Officer along with certain obligations. Simply put, it is an act designed to protect individual personal information both in the government and private sector by means of a National Privacy Commission.

This act is beneficial against the backdrop of competitors copying products, mirroring algorithms and pirating employees. As data is the only sustainable competitive advantage, it needs to be kept protected by means of fair laws that require mandatory compliance by organizations that are involved with handling personal data of any sort.

# Definitions

## Personal Data

This remains unchanged from its previous version. As per the draft, personal data is defined as "any data pertaining to a person that enables the identification of that person, whether directly or indirectly." However, data belonging to the deceased and information concerning private businesses are excluded from the Act.

## Data Controller

Any person, either natural or legal, with the decision-making authority regarding collection, usage or disclosure of personal data.

## Data Processor

Any person, either natural or legal, who with the orders of the data controller collects, uses or discloses personal data.

# Personal Data Protection Act: **What's Changing?**

Previously, Thailand did not have consolidated laws to govern data protection in general, despite certain business sectors such as banking, healthcare, telecommunications and credit bureaus already having specific laws in place.

However, with the implementation of the Personal Data Protection Act, the landscape of Thailand as far as personal data protection is concerned is going to change totally. It will be the very first consolidated law in Thailand to generally govern data protection.

Several other changes include the following:

| THEN | NOW |
|---|---|
| Data handlers had security clearance, privacy notices posted where appropriate (e.g. websites), use of data sharing agreements. | Prior to processing personal data in any way, it is imperative that data controllers - 'natural or juristic person' who has the power to make decisions regarding collection, usage or disclosure of personal data - get written or online consent from data subjects. |
| Differing concepts of "security incidents" and "personal data breaches" with the provision of not having to report all of the latter cases to the data subjects or the data protection authority. | Added protection to sensitive data. |
| Secure transfers were allowed, governed by each organizations' privacy management program and third-party agreements. | Restricted transfers to "Third Country". |
| Public and private sector companies within the Kingdom had to abide by the Act. | Laws are applicable to data controller companies outside Thailand if they use the countries' services |
| Each organization was expected to have a Data Protection Officer to ensure compliance. | Data controller representative with certain rights should be appointed by companies outside Thailand. |

# Breaking Down the Key Elements of Thailand's Personal Data Protection Act

Here are salient key elements of the Act:

## 1. Data owners' rights

According to the Act, data owners have the right to request access to personal data that concern them, except in cases where there are other laws governing the matter or court orders that apply. They may also request that their personal data be kept anonymous, suspended for a period of time, or destroyed altogether.

## 2. Data administrator's responsibilities

They are required to carry about their task of data collection according to the terms set by the law and should work well within the defined purposes for data collection. Data administrators should provide relevant details to data owners regarding the data that is being collected and obtain consent from them before doing so. The Act specifically mentions that data administrators must execute security measures to prevent any breach to the data like loss or alterations without authorization. Data owners should have access to their data on request.

## 3. Extra territorial reach

All those involved in data collection and processing of any sort, whether based in Thailand or elsewhere, are subject to the act if they offer services to Thai citizens or others within the country. To carry this out effectively, they are required to assign a local representative in the country and agree to the conditions that are outlined in the Act.

## 4. Consent

According to the draft, request for consent should be clear and not mislead data owners in any way. Such requests can either be made in writing or through digital means. Key factors that should be covered in such consents include the purpose of collection, what data is being collected and to whom it will be disclosed. There is scope for exceptions especially when involved parties are tied by contracts or if important interests are at stake. As far as parental consent is concerned, this is required for minors below 10 years of age and possibly even for those beyond that age under certain circumstances.

## 5. Third country data transfers

As per the Act, third country data transfers of personal data are not permissible as data protection regulations may be deficient in such countries. However, the following exceptions are allowed:

- In cases where consent has been obtained by the data owner after he or she is made fully aware of the insufficient data protection laws in the third country.
- In cases where certain obligations to a contract must be performed to which the data owner is a party.
- If the data owner does not have the capacity to give consent and the transfer of data is performed for the benefit of the data owner.
- Transfer is compliant with the contract between the data controller and data subject.
- In cases where another law requires it.

## 6. Protection of data

Procedures to secure personal data need to be implemented by data administrators. Certain guidelines may be produced by the committee and circulated to data administrators to help improve data protection practices. Also, the Committee may even grant the right to data administrators to display an official mark to indicate that the data administrators' data protection practices are certified as completely acquiescent by the Committee.

# Implications

The effect of the Personal Data Protection Act will have major implications both to businesses and individuals. Hence, companies and individuals should familiarize themselves with the details of the Act so as to abide by it, even in the smallest of ways. Failure to comply with the Act and any of its clauses will result in severe penalties as shown in the table below.

| TYPE OF FINE | FEES |
|---|---|
| Administrative Fines | Up to THB 5 Million |
| Criminal Fines | Up to THB 1 Million |
| Punitive Damages | Up to twice the damage caused and imprisonment for up to a year |

It is also worthy to note that failure to comply with the Act may result in both criminal and civil penalties. It is in the best interest of every company dealing with data collection or individual residing in Thailand, whether they are Thai citizens or foreigners, to get sound legal advice to fortify compliance with the new laws according to the Act.

# Key Steps for Addressing Thailand's Personal Data Protection Act Compliance

All companies should immediately check their internal data governance and work on taking action for compliance with the Act. Here are some key steps that should be taken:

## 1. Identify where data resides.

The first step in your data security strategy is to protect your sensitive data. To do this, determine where your most sensitive assets reside across your on-premises, cloud, and virtual environments. Search your file servers, applications, databases, and virtual machines for data at rest that must to be protected. And, don't forget to consider the network traffic flowing between your physical offices or other offsite locations. Once this data leaves the confines of your organization, you lose control over it. Attackers are ready to 'tap' the fiber optic cables, and human error can result in data transmission to the wrong location. Once you've located your sensitive data, encrypt it. Encryption is the critical last line of defense in the event of a breach because it applies protection and controls directly to your data and keeps it secure wherever it goes. Remember, encryption must be implemented properly to be effective. Be sure to also take steps to keep the encryption keys that can unlock your protected data safe too.

## 2. Own your sensitive data.

As the amount of data that you need to encrypt grows, so will the number of encryption keys. If you attempt to manage these keys in silos, it can leave them vulnerable to theft and misuse—especially if they are stored with the encrypted data or managed by a third party, such as a cloud service provider. The next step in your data security strategy is to centrally and securely manage and store your encryption keys. Enterprise key management provides a foundation for deploying encryption across your distributed organization. It enables you to centralize the management of important tasks including secure key generation, storage, rotation, back-up, and deletion. You also can define and control access to your protected information, ensuring you always maintain complete ownership and control of your protected data and keys. For an added layer of high-assurance security, consider storing your keys in a hardware security module (HSM). An HSM is a trust anchor that can securely manage, process, and store your cryptographic keys.

# 3. Control user access and polices.

Good encryption and key management will safeguard your sensitive data, but you also need to control who can access it. As your enterprise adopts new technologies such as mobile and cloud applications, increased controls are necessary. After all, relying on a simple user name and password is not an adequate method for protecting you, your company, your data, or your customers. The final step of your secure breach strategy is to control and manage access to your corporate resources. Access management enables you to verify a user's identity, assess and apply the appropriate access policy, and enforce the appropriate access controls using single sign-on.

Access management enables you to secure the breach by providing:

- Security: Apply the appropriate security policy for each access attempt and enforce the appropriate level of trust
- Visibility: Know which access controls are applied, track application usage, and know who is accessing which apps and when
- Scalability: Add new user groups, apps and policies as needed, eliminate help desk overhead associated with password resets, and centrally define access policies for all your cloud applications
- Convenience: Enable easy access through single sign on (SSO)

# Is your business ready for compliance?

Beyond the cyber-threat, an increasingly complex regulatory environment brings its own risks to businesses. Wherever you operate and whatever the regulation, Thales Cloud Protection & Licensing solutions can help with the following:

- Strengthen security: Eliminate islands of security and apply a unified strategy to manage access and secure data and identities.
- Achieve compliance and reduce audit costs: Get the visibility and holistic reporting you need to meet compliance and regulatory mandates.
- Reduce IT costs: Save time and money with proven security processes that can be scaled across your organization.
- Increase IT and business agility: With a centrally managed data security platform, IT becomes more nimble and can focus their efforts on new technology projects.

# Thales Cloud Protection & Licensing Compliance Solutions

Thales Cloud Protection & Licensing is a leader in providing solutions to the following compliance requirements we see in regulation after regulation around the world:

- Data access control
- Encryption and tokenization
- Encryption key management
- Keeping and monitoring user access logs
- The use of hardware security modules for executing encryption processes
- And, in some cases, encryption of data in motion

## Data Access Control

SafeNet Trusted Access is a cloud-based access management service that combines the convenience of cloud and web single sign-on (SSO) with granular access security. By validating identities, enforcing access policies and applying Smart Single Sign-On, organizations can ensure secure, convenient access to numerous cloud applications from one easy-to-navigate console.

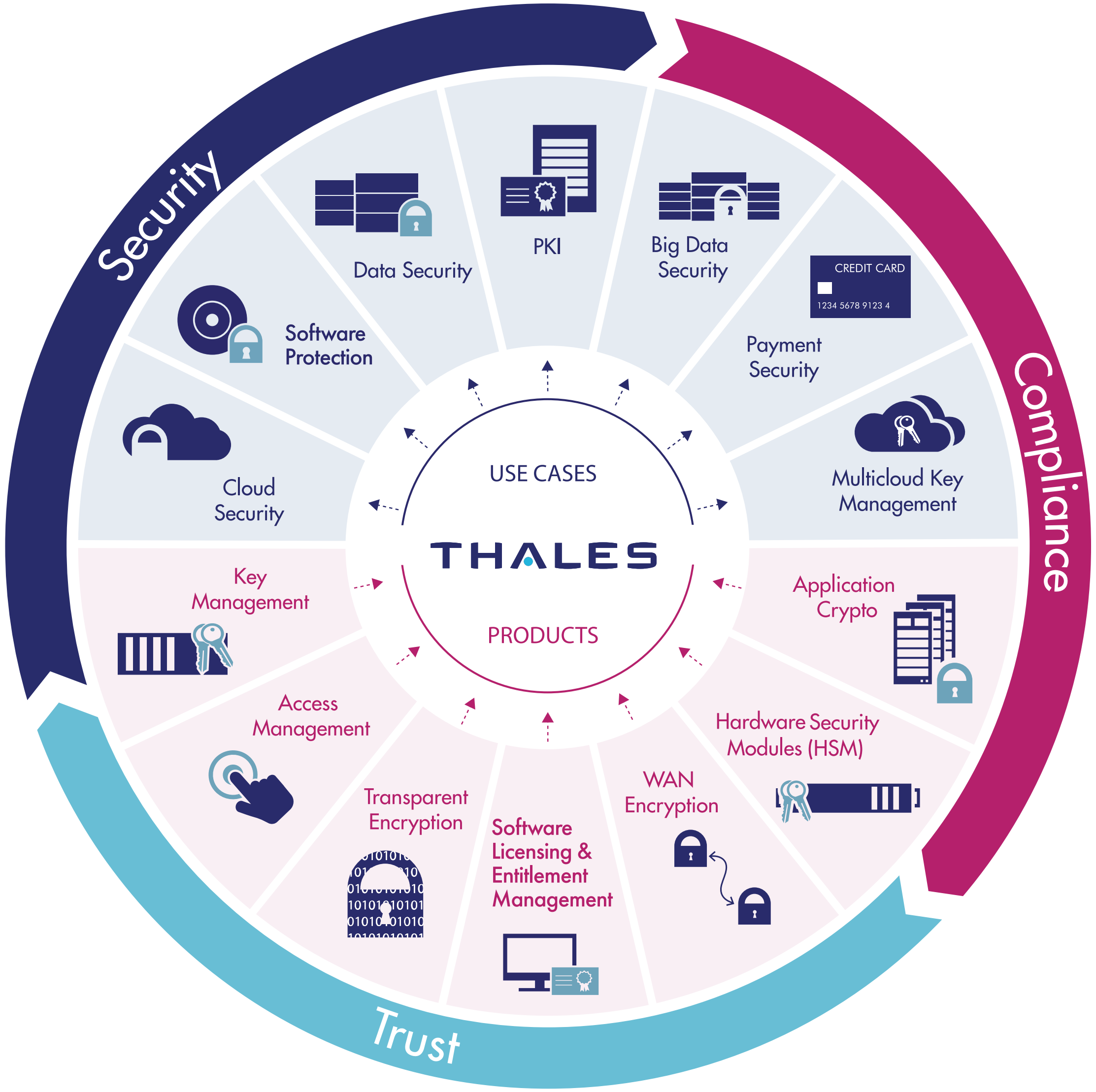
**SafeNet Trusted Access benefits:**

- Fast and easy cloud access through Smart Single Sign-On
- A single pane of glass for centralized user access control
- Optimized security through fine-grained access policies
- Visibility into all access events for simplified compliance
- Secure access for partners and contractors
- Identity-as-a-service efficiencies

# Encryption and Tokenization

The Vormetric Data Security Platform makes it easy and efficient to manage data-at-rest security across your entire organization. Built on an extensible infrastructure, the data security protection platform features multiple data security products that can be deployed individually or in combination to deliver advanced encryption, tokenization and centralized key management.

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 nimbly respond when the next security challenge or compliance requirement arises.



## The Vormetric Data Security Platform features these products:

- Vormetric Data Security Manager. The centralized management environment for all Vormetric Data Security Platform products. Provides policy control as well as secure generation, management and storage of encryption keys. Includes a Web-based console, CLI, SOAP and REST APIs. Available as FIPS 140-2 and Common Criteria certified virtual and physical appliances.
- Vormetric Transparent Encryption. Built around a software agent that runs on a server to protect data-at-rest in files, volumes or databases on-premises, in the cloud, or in hybrid cloud environments. Features hardware accelerated encryption, least-privilege access controls and data access audit logging across data center, cloud and hybrid deployments. Features these two extensions:
  - Container Security. Establishes controls inside of Docker™ and OpenShift™ containers, so you can ensure other containers and processes and even the host OS can't access sensitive data. Provides capabilities you need to apply encryption, access control and data access logging on a per-or within-container basis.
  - Live Data Transformation. Enables encryption and periodic key rotation of files and databases—even while in use—without disruption to users, applications and business workflows.
- Vormetric Tokenization with Dynamic Data Masking. Easy to implement format-preserving tokenization to protect sensitive fields in databases and policy-based dynamic data masking for display security.
- Vormetric Application Encryption. Streamlines the process of adding AES- 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 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.
- 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 storing certificates.
- CipherTrust Cloud Key Manager. Manages encryption keys for Salesforce Shield Platform Encryption, Mircosoft Azure Key Vault and AWS Key Management Services that addresses enterprise needs to meet compliance and best practices for managing encryption key life cycles outside of their native environments – and without the need for enterprises to become cryptographic experts. Available as a cloud service offering, or for private cloud or on-premises deployment.
- 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. Delivers pre-packaged 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.

# Hardware Security Modules

SafeNet Hardware Security Modules provide the highest level of security by always storing cryptographic keys in hardware. SafeNet Luna HSMs provide a secure crypto foundation as the keys never leave the intrusion-resistant, tamper-evident, FIPS-validated appliance. Since all cryptographic operations occur within the HSM, strong access controls prevent unauthorized users from accessing sensitive cryptographic material. Additionally, Thales also implements operations that make the deployment of secure HSMs as easy as possible, and our HSMs are integrated with SafeNet Crypto Command Center for quick and easy crypto resource partitioning, reporting and monitoring.

SafeNet HSMs adhere to rigorous design requirements and must pass through stringent product verification testing, followed by real-world application testing to verify the security and integrity of every device.

SafeNet HSMs are cloud agnostic, and are the HSM of choice for Microsoft, AWS and IBM, providing a "rentable" hardware security module (HSM) service that dedicates a single-tenant appliance located in the cloud for customer cryptographic storage and processing needs.

With SafeNet Hardware Security Modules, You Can:

- Address compliance requirements with solutions for Blockchain, GDPR, IoT, paper-to-digital initiatives, PCI DSS, digital signatures, DNSSEC, hardware key storage, transactional acceleration, certificate signing, code or document signing, bulk key generation, data encryption, and more.
- Keys are generated, and always stored in the intrusion-resistant, tamper-evident, FIPS-validated appliance, providing the strongest levels of access controls.
- Create partitions with a dedicated Security Office per partition, and segment through admin key separation.

Available in a wide range of form factors and performance options, SafeNet Luna General Purpose HSMs safeguard the cryptographic keys used to secure transactions, applications, and sensitive data.

#1

Worldwide in data encryption

Worldwide in key management

#1

Worldwide in general purpose HSMs

Worldwide in payment HSMs

Worldwide in cloud HSMs

# Payment HSM PayShield 10K

Thales Payment HSM PayShield 10K, the fifth generation of payment HSMs delivers a suite of payment security functionality proven in critical environments including transaction processing, sensitive data protection, payment credential issuing, mobile card acceptance and payment tokenisation. Like its predecessors over the past 30+ years, payShield 10K can be used throughout the global payment ecosystem by issuers, service providers, acquirers, processors and payment networks. Playing a fundamental security role for both face-to-face and digital remote payments, it delivers the necessary trust that underpins the communications between payments participants. payShield 10K addresses the latest mandated security requirements and best practices for a wide range of organizations including EMVCo, PCI SSC, GlobalPlatform, Multos, ANSI and the various global and regional payment brands and networks.

THALES

thalescpl.com

# About Thales Cloud Protection & Licensing

Today's enterprises depend on the cloud, data and software 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.

## References

https://silklegal.com/thailands-draft-personal-data-protection-act-a-preliminary-look/
https://silklegal.com/thailands-personal-data-protection-act-approved-as-law/
https://www.lexology.com/library/detail.aspx?g=5040828d-c80c-47aa-b6ef-06b9f4d1ea23
https://www.medianama.com/2019/06/223-thailands-personal-data-protection-act-is-in-effect-now/
https://www.bakermckenzie.com/en/insight/publications/2019/03/the-first-thailand-personal-data
https://www.dataprotectionreport.com/2018/08/overview-of-thailand-draft-personal-data-protection-act/
https://www.bakermckenzie.com/en/insight/publications/2019/05/thailand-personal-data-protection-act
https://www.bangkokpost.com/business/1678432/microsoft-advises-ai-regulation-under-pdpa

THALES Cloud Protection & Licensing, 12 Ayer Rajah Crescent, Singapore 139941 • E-mail: infoapac@gemalto.com

For More Information Please Contact:

DataOne Asia
Wholly owned by SVOA

**DataOne Asia(Thailand) Co.,Ltd.**
No.1023 MS Siam Tower, 30th Floor, Rama 3 Road, Chongnonsi, Yannawa, Bangkok 10120 Thailand.
Phone No.: +66 (0) 2686 3000 EXT.3843 l Email : d1.info@d1asia.co.th l Website : www.d1asia.co.th