Complying with Thailand's Personal Data Protection Act

Entrust helps enterprises comply with key requirements of Thailand's Personal Data Protection Act

- Secure personal data using a certified, tamper-resistant platform
- Protect legally shared personal data from disclosure
- Destroy personal data when retention periods end
- Prepare and maintain records of personal data processing

SUMMARY

Published in the Government Gazette, May 27, 2019, Thailand's Personal Data Protection Act (B.E. 2562 [2019]) addresses the collection, use and protection of personal data and puts in place remedial measures for data subjects whose personal data protection is violated. The PDPA applies to organizations located in Thailand, whether they collect and use the data in Thailand or not. It also applies to organizations located outside of Thailand if they offer goods and services to data subjects in Thailand, or if they conduct monitoring of data subjects' behavior in Thailand.

Thailand's PDPA is based on the EU's General Data Protection Regulation (GDPR), but it is not the same. So, being in compliance with GDPR does not ensure compliance with PDPA. Enterprises operating in Thailand or with Thai residents should review the PDPA to ensure compliance.

One way to ensure compliance is to make sure personal data your organization holds is protected through cryptographic pseudonymization techniques, such as tokenization, and that the underpinning cryptographic keys are protected by storing and managing them in FIPS and Common Criteria certified Entrust nShield® hardware security modules (HSMs).

Following are excerpted parts of Thailand's PDPA that Entrust can help you comply with.

Complying with Thailand's Personal Data Protection Act

PDPA Regulations	Entrust Solution
Section 37--The Data Controller shall have the following duties:	
1. Provide appropriate security measures for preventing the unauthorized or unlawful loss, access to, use, alteration, correction or disclosure of Personal Data... 2. In the circumstance where the Personal Data is to be provided to other Persons or legal persons, apart from the Data Controller, the Data Controller shall take action to prevent such person from using or disclosing such Personal Data unlawfully or without authorization; 3. Put in place the examination system for erasure or destruction of the Personal Data when the retention period ends, or when the Personal Data is irrelevant or beyond the purpose necessary for which it has been collected, or when the data subject has request to do so, or when the data subject withdraws consent...	• The customized tokenization solution from Entrust Professional Services converts plain text data to tokens that cannot be traced back to the original data. • Stolen tokens cannot be reversed without access to the Entrust solution. • Altered tokens cannot be used to recreate the original data. • The Entrust solution can partially mask data before sending it to third-party entities to maintain data confidentiality. • The solution authenticates legitimate users to prevent unlawful users from gaining plaintext data. • Tokens are based on cryptographic keys protected in Entrust nShield HSMs. • Upon retention expiry of data, token keys can be removed from nShield HSMs. • Without token keys, tokens cannot be de-tokenized – ensuring retired data invalidity.
Section 40--The Personal Data Processor shall have the following duties:	
3. Prepare and maintain records of personal data processing activities in accordance with the rules and methods set forth by the Committee.	• The Entrust solution provides logs of tokenization, de-tokenization and masking calls for audit reference.
Section 42--The data protection officer shall have the following duties:	
4. Keep confidentiality of the Personal Data known or acquired in the course of his or her performance of duty under this Act. The Data Controller or the Data Processor shall support the data protection officer in performing the tasks by providing adequate tools or equipment as well as facilitate the access to the Personal Data in order to perform the duties.	• The Entrust solution tokenizes data to maintain confidentiality. • Access to Entrust solution is limited to users who hold the cryptographic keys credentials. The Data Protection Officer can obtain personal data with application de-tokenization calls using the correct key secret.

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

Learn more at
entrust.com/HSM

Contact us:
HSMinfo@entrust.com