blancco

How Does Blancco Help Organizations Comply with Thailand's Personal Data Protection Act (PDPA)?

The Thai Personal Data Protection Act (PDPA), B.E. 2562 (2019), sets rules around how companies should collect, use, share, and dispose of personal data. To comply with the law, organizations must destroy or anonymize data when they no longer need it, like when the retention period ends or when someone asks for their data to be removed.

This document explains how to follow the PDPA by fully erasing data that is no longer needed.

What is the PDPA, and who must follow it?

The PDPA is Thailand's main law about data privacy. It took effect on June 1, 2022, and has been updated since then to make data protection rules stronger. The law controls how businesses handle personal data and protects the privacy of Thai citizens.

The PDPA applies to anyone who collects, uses, shares, or transfers personal data in Thailand for business purposes. This includes:

- data controllers and processors in Thailand, and
- businesses outside of Thailand offering goods or services to individuals in Thailand or monitoring their online behavior.

Some exceptions apply, such as for government activities or other specific cases.

What does the PDPA require?

The PDPA is similar to Europe's GDPR, but with some differences. Here are the law's key rules:

Consent
Businesses must get permission before collecting personal data unless the law allows it for certain tasks, like public interest activities or fulfilling a contract.

In most cases, businesses need clear consent from the person whose data they are collecting.

Data accuracy
Businesses must keep personal data accurate and up-to-date. People can ask businesses to fix incorrect information.

Record keeping and small businesses
Small- and medium-sized businesses may not have to keep detailed records of how they process data unless they handle sensitive data or create risks for individuals' rights.

Security measures
Data controllers should review their security as technology changes, or as needed.

Data retention
Businesses must tell people how long they will keep their data.

After this time, the data must be deleted, destroyed, or anonymized, unless there are special reasons to keep it longer.

Data breach reporting
Data breaches should be reported to the authorities within 72 hours unless certain conditions apply.

Penalties for breaking the rules

The Personal Data Protection Committee (PDPC) enforces the law and publishes guidelines. Breaking the PDPA can lead to criminal, civil, or administrative penalties. Serious violations, like leaking sensitive data, could lead to prison time or fines.

For example, in November 2024, an online sales company was fined 7 million baht ($204,000 USD) for not following the rules. The company was fined for several issues, including not appointing a data protection officer or having proper security measures.

blancco

Data disposal under the PDPA

All organizations that collect, use, or transfer data will eventually need to dispose of it. If they do not do this safely, the data could be accessed by unauthorized people. The PDPA says that data must be safely removed when:

- The retention period ends,
- The data is no longer needed for its original purpose, or
- A person asks for their data to be removed.

The PDPC has issued rules about how data should be deleted, destroyed, or anonymized (Notification on Criteria for Deletion, Destruction or Anonymization of Personal Data, B.E. 2567 (2024). These rules took effect on November 11, 2024, and include:

- **Deadlines:** Businesses have 90 days to delete, destroy, or anonymize data after someone requests it. If businesses can't meet the 90-day deadline, they must limit access to the data until it can be properly destroyed.
- **Standards:** Data must be disposed of in a way that makes it impossible to recover or re-identify. This includes backups.
- **Choice:** People can also ask for specific disposal methods, but businesses must choose a compliant method and inform the person. If the data subject files a request for data that was unlawfully processed, de-identification is not allowed. In that case, the data controller must use deletion or destruction techniques.

> **Data controllers must ensure that personal data directly or indirectly identifying data subjects is deleted, destroyed, or anonymized so that it cannot—through reasonably foreseeable means—be recovered or serve to re-identify the data subject.**

The following section explains what the terms "deleted" and "destroyed" mean. We also share details on the most secure, compliant way to remove data—erasure.

blancco

Data deletion, destruction, and erasure

Many regulations use words such as data "deletion," "destruction," and "erasure," but it's important to look beyond this so you know how to comply with the intent of these laws:

Data deletion. Deletion simply means getting rid of data. But many operating systems and applications have a "delete" button that does not remove data completely. It moves it from one place to another. A skilled user with the right software could still find this data. To know that the data you are "deleting" is truly gone, we recommend software-based data sanitization, or data erasure.

Data destruction is also a general term. Data can be destroyed in several ways, but unless it is verified and certified, there is no way to prove that data has been completely eliminated.

Data erasure. This is a software-based process of securely overwriting digitally stored information with random binary data according to a specified standard, then verifying and certifying that the erasure has been successful. With data erasure, overwritten data cannot be recovered.

What does the PDPA ask you to do?

Thailand's Personal Data Protection Act says that data should not be recoverable after its permitted lifespan. Data erasure is the guaranteed, effective way to do this because no one can recover it afterwards.

Businesses must also keep proof that data has been deleted or destroyed in case of audits. While some data destruction methods lack traceable evidence, certified erasure reports and documented audit trails give full confidence in the way you manage your end-of-life data.

How Blancco can help

Blancco offers a range of solutions to erase data across your entire range of data storage assets and ensure compliance with PDPA data destruction requirements.

Blancco Hardware Solutions
Secure, on-premise erasure of loose drives and drive enclosures within data centers or large IT facilities

Blancco Drive Verifier
Secure drive erasure verification for PCs, laptops, and loose drives

Blancco Mobile
Diagnostics and secure data erasure of smartphones and tablets

Blancco LUN Eraser
Secure data erasure of LUNs in an active storage environment, connected to both physical and virtual machines

Blancco Management Portal
Centralized data erasure reporting and management across your entire IT asset portfolio – on-premise or in the cloud

Blancco Drive Eraser
High speed, efficient secure data erasure of complex SSD and NVMe drives, including self-encrypting drives

Blancco Virtual Machine Eraser
Secure data erasure of complicated server and storage environments

Blancco Removable Media Eraser
Secure data erasure of removable flash media devices stored within smartphones, tablets, network routers, and cameras

Blancco File Eraser
Secure data erasure of files and folders on active PCs, laptops, and servers

To see how Blancco data erasure solutions work to keep you compliant, request a free Enterprise trial of Blancco data erasure software today.

You may also contact Blancco Thailand: Khun Siripan Na Jatturat, siripan.jatturat@blancco.com.