ORRADATA

Thailand's Personal Data Protection Act (PDPA)

Simplified Explanation

A concise overview of principles, rights, and compliance requirements

www.orradata.com

Summary

Thailand's **Personal Data Protection Act B.E. 2562 (2019)**, fully enforced on June 1, 2022, is the country's first consolidated law governing data privacy, designed to align Thailand's digital economy with international standards like the GDPR. It regulates how "Data Controllers" and "Data Processors" handle personal information, establishing a consent-based framework with specific lawful exceptions and granting individuals extensive rights, such as the right to access, object, and delete their data. The Act applies extraterritorially to foreign entities offering goods or services to individuals in Thailand and introduces a strict three-tiered penalty regime—comprising administrative fines, criminal imprisonment for unauthorized disclosure of sensitive data, and civil punitive damages—overseen by the **Personal Data Protection Committee (PDPC)**.

1. Overview & Timeline

- The **Personal Data Protection Act B.E. 2562 (2019)** was published in the Royal Gazette on **May 27, 2019** and became fully enforceable on **June 1, 2022**
- It applies broadly—covering both **data controllers and processors** based in Thailand, or those offering goods/services or monitoring individuals in Thailand

2. Key Definitions & Scope

- **Personal Data**: Any information about an identifiable natural person, whether direct or indirect. Excludes data on deceased individuals
- **Controller & Processor**: A **controller** decides why and how data is processed, while a **processor** acts on behalf of the controller
- Exemptions apply for household activities, media, arts, academic uses, and certain state security/public safety operations by government authorities

3. Lawful Bases for Processing & Consent

- PDPA sets **six legal bases** for lawful processing
    1. Public interest or archival/research purposes
    2. Vital interests (e.g. to protect life or health)
    3. Contract performance
    4. Tasks in the public interest or official duties
    5. Legitimate interests (unless overridden by rights)
    6. Legal obligation
- **Consent** must be explicit (written or electronic), informed (clear, separate, non-misleading), and obtained prior to processing. Withdrawal of consent must be equally easy

4. Notification (Privacy Notice)

Before or at the point of data collection, organisations must notify the data subject about:

- What data is collected
- Purpose and legal basis
- Retention period or expected duration
- Recipients (e.g. categories)
- Contact details (controller, representative, or DPO)
- Rights available to the data subject

5. Core Obligations of Controllers & Processors

Controllers must:

- Apply **data minimization**: collect only necessary data
- Ensure **purpose limitation**: process data only for notified and lawful purposes
- Keep data **accurate, complete, and up to date**
- Implement **adequate technical and organizational security measures**, reviewed as needed with changing technology
- Maintain **records of processing activities (RoPA)**—required for most organisations, with exemptions for small SMEs in low-risk cases
- Respond appropriately to data subject rights requests

Processors must follow controller instructions, secure data, and also keep records where applicable.

6. Rights of Data Subjects

Data subjects can exercise these rights under the PDPA:

- **Right to be informed**
- **Right of access** (copy of their data)
- **Right to rectification** (fix errors)
- **Right to erasure ("right to be forgotten")**
- **Right to restrict processing**
- **Right to data portability** (structured machine-readable transfer)
- **Right to object** to processing
- **Right to withdraw consent**
- **Right to lodge a complaint** with the regulator (PDPC)

Where valid grounds exist, organisations may refuse certain requests.

7. Cross-Border Data Transfers

Transfers of personal data outside Thailand are allowed only if:

- The destination country ensures **adequate data protection**, or

- An exemption applies (such as explicit consent, contractual necessity), or
- Certified intra-group transfer policy is approved by the PDPC

8. Data Breach Notification

- Reports must be made **to the PDPC within 72 hours** of becoming aware of a breach, unless it poses no risk to individuals
- If a breach poses **high risk**, the controller must also notify affected data subjects without delay and communicate remedial actions

Processors must notify controllers of breaches.

9. Appointment of Data Protection Officer (DPO)

A **DPO** must be appointed if:

- The organisation is a public authority,
- Performs large-scale systematic monitoring, or
- Handles large-scale sensitive personal data

The DPO ensures PDPA compliance and interacts with the PDPC and data subjects.

10. Enforcement & Penalties

Violations can lead to:

- **Administrative fines** up to THB 5 million (≈ USD 140,000)
- **Criminal penalties** for severe breaches: prison up to 1 year and fines up to THB 1 million
- **Civil liability**, including punitive damages up to twice the actual harm suffered by data subjects

Illustrative case: In **July 2024**, a Thai IT company was fined **THB 7 million**: THB 1 M for not appointing a DPO; THB 3 M for weak security; THB 3 M for delayed breach reporting. The company was also ordered to overhaul its data protection framework and report weekly to the PDPC.

11. Summary Table

Area	Key Requirement
Lawful Basis	Consent or other legal grounds (e.g. contracts, public interest)
Consent	Explicit, informed, documentable, and withdrawable
Notification	Privacy notice before or at data collection
Data Rights	Rights to access, rectify, erase, object, export, restrict, withdraw consent
Controllers & Processors	Record-keeping, data minimization, purpose limits, accuracy, security, breach response

DPO	Required for public authorities or high-volume/sensitive processing
Cross-Border Transfers	Allowed only with adequate protections or appropriate safeguards
Breach Notification	Report to PDPC within 72h; notify subjects if high risk
Enforcement	Fines, criminal charges, civil lawsuits

Disclaimer:
This document is provided for general informational purposes only. It offers a simplified overview of Thailand's PDPA and does not constitute legal advice. Organizations and individuals should consult official regulatory texts or seek professional legal counsel for advice regarding their particular obligations under the PDPA.