Newsletter:

An Overview of Personal Data Protection Law in Thailand

In Brief

In Thailand, personal data protection is governed by the Personal Data Protection Act B.E. 2562 (2019) (the **"Personal Data Protection Act"**), which has been fully enforced since June 1, 2022. Its purpose is to prevent personal data breaches by setting standards for personal data protection and defining the duties of individuals or business entities involved in the collection, use, or disclosure of personal data (the "**Data Controller**" and "**Data Processor**") under the Personal Data Protection Act.

One key duty of both Data Controllers and Data Processors is to respect the rights of data subjects, including customers, employees, and business partners ("**Data Subject**"). For example, personal data may only be collected, used, or disclosed for the purpose to which the Data Subject has given explicit consent.

In addition, failure to comply with the provisions of the Personal Data Protection Act may result in penalties for both Data Controllers and Data Processors.

Personal data under the protection of the Personal Data Protection Act

Personal Data means any information that can identify an individual (identify the owner of the information), whether directly or indirectly and personal data can take the form of documents, paper, books, or be stored electronically. It can be divided into 2 types:

1) General Personal Data such as name, address, phone number, photo, etc. as a basic personal data.
2) Sensitive Personal Data such as race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal history, health information, disability or mental health information, etc.

However, personal data of deceased persons or information of legal entities such as companies, foundations, associations, organizations are not considered personal information under the Personal Data Protection Act.

Key Steps in the Event of a Personal Data Security Measures Breach

Under Section 37(4) of the Personal Data Protection Act, in the event of a breach of personal data security measures that results in the loss, access, use, alteration, modification or disclosure of personal data without authorization, the Data Controller is required to notify the Personal Data Protection Committee ("**PDPC**") of a personal data security measures breach within 72 hours of becoming aware of the incident, and to notify affected Data Subjects if the breach poses a high risk to the rights and freedoms of Data Subjects. The Data Controller must provide a notification with details of the breach and the corrective measures taken ("**Incident Notification**"), unless the breach does not pose a risk to the rights and freedoms of Data Subjects, for example, the personal data is no longer in a usable form because the effective technological measures have been applied. In this case, the data controller is still obligated to submit relevant information, documents, or evidence concerning the incident to the PDPC for consideration as to whether the rights and freedoms of the Data Subject are impacted.

Author


Tanadee Pantumkomon
Partner
Tanadee.P@ilawasia.com


Nannapas Phatcharakeatkanok
Senior Associate
corporate@ilawasia.com


Wachinorot Siladet
Associate
corporate@ilawasia.com


Kamintra Piriyayon
Associate
corporate@ilawasia.com

Contact

ILAWASIA CO., LTD.
319 Chamchuri Square Building,
Floor 17th, Unit 1702, Phayathai Road,
Pathumwan Sub-district,
Pathumwan District, Bangkok, 10330
Thailand
Tel:+66 (0) 2 048 2534
Email: info@ilawasia.com

About Us

ILAWASIA is a full-service, Thai law firm based in central Bangkok. Mr. Somphob Rodboon, an acclaimed expert in business law and litigation in Thailand, founded ILAWASIA since 2007. A visionary Managing Partner, he expanded the firm's operation into Myanmar through acquisition of an experienced and respected local law firm in June 2018. Additionally, the firm established an office in Cambodia in August 2019 and incorporated a branch in Laos in January 2021.

We offer services in business and international law ranging from corporate and commercial law, litigation, intellectual property and due diligence to immigration, real estate and labour law. Our teams are individualistically experienced in legal practice and always combine cutting-edge understanding with a unique sensitivity to international clients' business needs. With pride, we take our ethical standards seriously, ensuring responsibility, care and respect in all aspects of our operations.

Key Steps in the Event of Non-compliance by Data Controller and Data Processor

If Data Controller and Data Processor fails to comply with the provisions of the Personal Data Protection Act, Data Subjects have the right to file a complaint to the Expert Committee under Section 73 of the Act.

The Expert Committee will then assess the complaint to determine its seriousness and issue an order based on the severity. The possible outcomes include:

1) Mediation: If the Expert Committee determines that the complaint can be resolved through mediation, and both parties agree, a mediation process may be initiated.
2) Warning: If the complaint is not considered serious, the Expert Committee may issue a warning to the Data Controller and Data Processor, or require the Data Controller and Data Processor to remedy or resolve the issue, or to cease, suspend, or refrain from the non-compliant action.
3) Administrative Fine: If the complaint is deemed serious, or if the Data Controller and Data Processor fail to comply with a prior warning, the Expert Committee has the authority to impose an administrative fine on Data Controller and Data Processor.

However, apart from filing a complaint with the Expert Committee above, Data Subject also has the right to file a lawsuit against the Data Controller in court to claim compensation, even without filing a complaint with the Expert Committee.

Doxxing as a Criminal Offense

With the rise of social media, users often share personal details online, creating vast digital footprints. Unfortunately, this information can be accessed, collected, and redistributed without the Data Subject's consent. Doxxing refers to the malicious act of publicly disclosing a Data Subject's private information, such as their name, address, phone number, or other sensitive details, with the intent to harm, harass, or embarrass them.

Under the Personal Data Protection Act, disclosing sensitive personal data without the Data Subject's explicit consent, or using such data for purposes other than originally intended, is illegal. This includes the act of doxxing, which is considered a violation of the individual's rights to privacy and security.

Importantly, doxxing can lead to criminal penalties under the law. If the disclosure of personal data results in harm, damage to the Data Subject's reputation, or causes insult or embarrassment, it is considered a criminal offense.

Penalties under the Personal Data Protection Act

In the event of a personal data breach, the following penalties may apply:

A. Civil Compensation

If the Data Controller and Data Processor fail to comply with the provisions of the Personal Data Protection Act, whether due to intentional actions or negligence, they may be required to compensate the Data Subject for actual damages caused by the breach. In addition, they may be subject to punitive damages of up to twice the actual damages, unless the Data Controller or Data Processor can prove that:

1) The damage was caused by force majeure or resulted from the Data Subject's own actions or omissions.
2) The action was carried out in compliance with an official order issued within lawful authority and duty.

For example, if the court rules that the Data Controller and Data Processor must pay 100,000 Baht in compensation to the Data Subject, the court may order additional punitive damages of up to twice of the actual damages, meaning the total amount payable would be 200,000 Baht.

Penalties under the Personal Data Protection Act (cont.)

B. Criminal Penalties

1) If the Data Controller uses or discloses sensitive personal data without the Data Subject's consent or uses the data for purposes other than those originally disclosed, causing harm, damage to reputation, insult, or embarrassment to the Data Subject, they may face imprisonment for up to 6 months, a fine not exceeding 500,000 Baht, or both imprisonment and a fine.

2) The action was carried out in compliance with an official order issued within lawful authority and duty.

In cases where the offender is a legal entity (juristic person), executives, directors, or other persons responsible for the company's operations may be jointly liable with the company.

C. Administrative Penalties

The law specifies fines ranging from 500,000 Baht to 5,000,000 Baht, for failure to comply with the Personal Data Protection Act, including:

1) Improper use or disclosure of data.

2) Improper transfer of sensitive personal data abroad.

3) Failure to comply with the orders of the Expert Committee, failure to provide required explanations, or failure to submit necessary information to the Expert Committee.

Please note that civil compensation, criminal penalties, and administrative penalties are separate and can be imposed independently.

Conclusion

The Personal Data Protection Act establishes crucial mechanisms for addressing personal data breaches and ensuring compliance by Data Controllers and Data Processors.

Key obligations include the prompt notification of data breaches to the PDPC within 72 hours and filing complaints in cases of non-compliance. These mechanisms are designed to protect personal data rights and ensure accountability in data processing activities.

At ILAWASIA, we offer expert legal counsel on the Personal Data Protection Act compliance, including litigation process for any breach under the Personal Data Protection Act, assisting businesses in navigating their regulatory obligations with confidence. If you need guidance on incident notification, filing complaints, or any other the Personal Data Protection Act-related matters, please contact us for further consultation.

Recognitions

Recognized as one of 30 firms in ALB 30 Fastest Growing Firms in 2024.

Recognized as one of Notable firms in ALB M&A Ranking 2024.

Recognized as one of eight finalists of regional IP firms of year 2024 - 2025.

Ranked in the Thailand Law Firm Awards 2024 in Labour & Employment category, assessed by Asia Law Business Journal.

Ranked in the Thailand Law Firm Awards 2025 in Healthcare & Lifesciences category, assessed by Asia Law Business Journal.

Benchmark Litigation Asia-Pacific has appraised ILAWASIA as Recommended Firm for consecutive terms. Furthermore, ILAWASIA is ranked in tier 3 for "Commercial and Transactions" category. Also ranked as 'Notable Firms' for "Government and Regulatory," "Intellectual Property," and "Trade and Customs" during 2023-2024.

Ranked in the Asian Legal Business (ALB) for Asia IP Rankings in 2022 - 2024.

Recognized as d-lawfirm Membership of the Digital Economy Promotion Agency (depa) of Thailand, effective April 2023, to April 2026.

Honored as the Best Modern Full-Service Law Firm in Thailand for 2024 in the Corporate Excellence Awards, as surveyed by Corporate Vision magazine, issue 6/2024.

Our Offices

Bangkok, Thailand
ILAWASIA CO., LTD.
Operated since 2007 to present.

Yangon, Myanmar
ILAW MYANMAR CO., LTD.
Operated since 2018 to present.

Vientiane, Laos
ILAW LAOS CO., LTD.
Operated since 2021 to present.

Phnom Penh, Cambodia
I.L. ASIA CO., LTD.
Operated since 2019 to present.

Phnom Penh, Cambodia
ILAW CAMBODIA LAW OFFICE
Operated since 2023 to present.

Singapore
ILAW SINGAPORE PTE. LTD.
Operated since 2023 to present.