

Legal Update: PDPA Enforcement Intensifies Key Cases, Risks, and Compliance Insights

24th October 2025
OAL Thailand Office
Praow Panyasereeporn
Miho Marsh

Since the full enforcement of the **Personal Data Protection Act 2019** (“PDPA”) on 1st June 2022, the **Personal Data Protection Committee** (“PDPC”) has transitioned from a phase of awareness and implementation to one of active enforcement. In 2024, a leading technology retailer was fined a substantial amount, marking a significant milestone in the evolution of PDPA enforcement. These developments underscore that compliance with the PDPA is no longer discretionary and constitutes a binding legal obligation, with breaches potentially resulting in substantial financial penalties and reputational consequences.



1. Legal Framework for Sanctions

1.1 Civil Liability

Data Controllers or Data Processors who unlawfully process personal data, causing damage either intentionally or negligently, may be required to compensate data subjects. Furthermore, the court has the authority to order punitive damages of up to twice the amount of the actual losses incurred, in addition to the aforementioned compensation.

1.2 Criminal Liability

Violations, particularly those that may cause sustain damage or defamation to others, or involve accessing personal data (especially sensitive personal data) and unlawfully disclosing it during the course of duty shall be punishable by imprisonment for not more than six months, a fine not exceeding 500,000 baht, or both. Furthermore, if the above violations are committed for the purpose of obtaining unlawful gain for oneself or a third party, the offender shall be liable to imprisonment for not more than one year, a fine not exceeding one million baht, or both. Directors and executives of legal entities may also be held personally liable.

1.3 Administrative Sanctions

The Experts Committee designated under the Office of the PDPC may impose administrative fines of up to THB 5 million per contravention and also retains discretion to issue warnings or order corrective measures in lieu of monetary penalties.

2. Recent Enforcement Cases

To date, five significant cases had concluded with total administrative fines exceeding THB 14 million across public and private entities, as detailed below:

No.	Entity / Role	Nature of Violation	Legal Basis	Administrative Fine (THB)
1.	Government Agency (Data Controller) / Private Vendor (Data Processor)	A government agency outsourced the development of its web application to a private vendor without executing a Data Processing Agreement (“DPA”). The agency relied on weak passwords, conducted no risk assessments, and failed to implement fundamental	Section 37(1): Failure to implement adequate technical and organizational measures to protect personal data against unauthorized access, loss, or disclosure. Section 37(5): Failure of Data Controllers to	Both the Government Agency and the Private Vendor were fined THB 153,120 each in the incident.



		information security measures. Consequently, the system was compromised, leading to the unauthorized sale of over 200,000 citizens' records on the Dark Web.	ensure that Data Processors provide sufficient guarantees of appropriate safeguards for the processing of personal data	
2.	Large Private Hospital (Data Controller) / Contractor Employee (Data Processor)	A private hospital engaged a contractor to destroy sensitive health records but failed to adequately supervise or monitor the process, resulting in the unauthorized disclosure of over 1,000 patient records. It was found that an employee, who had deleted the data, detected the breach but did not report it as required.	Section 26 Paragraph 1: Processing of sensitive personal data without a legal basis or without complying with specific statutory requirements. Section 37(1): Failure to implement adequate technical and organizational measures to protect personal data against unauthorized access, loss, or disclosure.	The Private Hospital was fined THB 1,210,000 , while the Contractor Employee was fined THB 16,940 in the incident.
3.	Technology Retailer (Data Controller)	A major technology retailer failed to appoint a Data Protection Officer ("DPO"), neglected to implement appropriate security safeguards, and did not notify the PDPC of a personal data breach.	Section 37(1): Failure to implement adequate technical and organizational measures to protect personal data against unauthorized access, loss, or disclosure. Section 37(4): Failure to notify the PDPC of a personal data breach within seventy-two hours of becoming aware of the incident. Section 41: Failure to appoint a DPO where processing involves large-scale sensitive data or requires regular monitoring of personal data.	The Technology Retailer was fined THB 7 million in the incident, consisting of THB 3 million for failing to implement appropriate security measures, THB 3 million for failing to notify the Personal Data Protection Committee of the data breach, and THB 1 million for failing to appoint a DPO and negligently failing to remedy the issue, which was deemed a serious violation of acceptable business practices.
4.	Cosmetics Company (Data Controller)	A cosmetics company experienced a data breach that was subsequently linked to fraudulent activity within its call center. The company failed to implement adequate technical and organizational safeguards, did not notify the PDPC of the incident, and offered no remedial	Section 37(1): Failure to implement adequate technical and organizational measures to protect personal data against unauthorized access, loss, or disclosure. Section 37(4): Failure to notify the PDPC of a	The Cosmetics Company was fined in the THB 2.5 million in the incident.

		measures to the affected individuals.	personal data breach within seventy-two hours of becoming aware of the incident.	
5.	Global Toy Retailer (Data Controller) / External Vendor (Data Processor)	A global toy retailer was sanctioned following the hacking of its outsourced online reservation system. Neither the retailer nor the vendor had implemented sufficient security measures. While the retailer acted promptly to mitigate harm to data subjects, the vendor failed to respond in a timely manner or provide redress.	Section 37(5): Failure of Data Controllers to ensure that Data Processors provide sufficient guarantees of appropriate safeguards for the processing of personal data Section 40: Failure of Data Processors to maintain appropriate data protection standards during the processing of personal data.	Global Toy Retailer was fined THB 500,000 , while External Vendor was fined THB 3 million in the incident.

In addition to the above, recent enforcement actions highlight violations ranging from personal data leaks due to large-scale unauthorized access at major corporations to the unauthorized use of personal data. Major entities like Bangchak and Thailand Post are under investigation for exposing millions of customer records due to inadequate security measures. Furthermore, in cases based on complaints alleging unauthorized use of former employees' data or its continued use for marketing purposes after consent has been withdrawn, the PDPC has issued warnings and corrective orders to first-time offenders. These cases demonstrate that the PDPC is actively enforcing compliance through a broad spectrum of measures, ranging from ordering corrective actions to conducting investigations with a view to potential administrative fines.

3. Conclusion



Recent PDPC enforcement actions demonstrate that compliance with the PDPA is mandatory and carries significant financial, legal, and reputational consequences. High-profile cases show that both Data Controllers and Data Processors, as well as potentially individual employees, can be held liable for inadequate security measures, failure to notify breaches, or insufficient oversight of vendors. Organizations must adopt proactive data protection practices, including robust security frameworks, formalized breach response protocols, comprehensive Data Processing Agreements, and, where required, the appointment of a Data Protection Officer. Embedding these measures not only mitigates regulatory risk but also reinforces stakeholder trust and safeguards organizational reputation.

Should you have any questions or require further clarification regarding PDPA compliance, please do not hesitate to contact One Asia Lawyers (Thailand Office), where our team will be pleased to assist you.

◆ One Asia Lawyers ◆

One Asia Lawyers Group is a network of independent law firms created to provide seamless and comprehensive legal advice for Japanese and international clients across Asia. With our member firms in Japan, Southeast Asia, Oceania and other ASEAN countries, One Asia Lawyers Group has a strong team of legal professionals who provide practical and coherent legal services throughout each of these jurisdictions. For any enquiry regarding this article, please contact us by visiting our website: <https://oneasia.legal> or email: info@oneasia.legal. This newsletter is general information for reference purposes only and therefore does not constitute our group member firm's legal advice. Any opinion stated in this newsletter is a personal view of the author(s) and not our group member firm's official statement. Please do not rely on this newsletter but consult a legal adviser or our group firm member for any specific matter or legal issue. We would be delighted to answer your questions, if any.

<Author>

	<p>Praow Panyasereeporn One Asia Lawyers Thailand Office Attorney at law in Thailand</p> <p>Her practice focuses primarily on corporate law, data protection, and intellectual property. She handles a wide range of corporate matters, from structuring and negotiating commercial agreements and advising on investment promotion incentives to conducting thorough legal due diligence. She also has extensive experience in data privacy, advising on PDPA compliance from the implementation stage. Furthermore, her work includes providing multinational clients with customized training on key compliance topics such as anti-bribery, corporate compliance, and whistleblowing systems.</p> <p>praow.p@oneasia.legal</p>
	<p>Miho Marsh One Asia Lawyers Thailand Office Director</p> <p>In collaboration with Thai lawyers, she provides advice on a wide range of legal matters, focusing primarily on corporate, labor, and compliance fields. In the corporate sector, she handles a broad spectrum of issues, from various license applications—including those related to foreign ownership restrictions, BOI, and the Foreign Business License (FBL)—to complex corporate legal matters such as mergers, dissolutions, and liquidations. She also has extensive experience in labor law, handling cases ranging from general employment issues to labor litigation. Furthermore, her responsibilities include conducting compliance audits, advising on inheritance and real estate transactions, and assisting with the establishment of external whistleblowing systems.</p> <p>miho.marsh@oneasia.legal</p>