



TMI Eyes No. 17: Lessons from the First Administrative Fine under Thailand's PDPA

Readers may be aware of the first-ever case under Thailand's Personal Data Protection Act B.E. 2562 (2019) (PDPA). In this article, TMI decodes the factual background and cause of the fine, providing valuable insights to help companies avoid similar mistakes and strengthen their data protection measures.

The First-Ever Fine

In August 2024, the Ministry of Digital Economy and Society (MDES) and the Second Expert Committee ("Committee") under the Office of the Personal Data Protection Commission (PDPC) imposed the first-ever administrative fine under Thailand's PDPA. The data controller, an online trading business, was penalized for multiple violations of the PDPA and fined a total of THB 7,000,000.

PDPA Violations

TMI provides the background and key violations for readers to use them as their own health check.

1. DPO Appointment

The data controller failed to appoint a **Data Protection Officer (DPO)**. It is crucial for readers to know when a DPO must be appointed. According to the PDPA, a DPO is required when the data controller:

1. (i) Collects, uses, or discloses personal data as part of its core activities, which (ii) regularly and systematically monitor data subjects (e.g., tracking online behavior or processing customers' data on a mass scale); (iii) because of having large volumes of personal data (e.g., more than 100,000 data subjects); or
2. Collects, uses, or discloses sensitive personal data as its core activities.

In this case, the Committee found that the data controller had collected and used the personal data of over 100,000 customers as part of its core profit-seeking business activities. Thus, the data controller was obligated to appoint a DPO but failed to do so. As a result, the Committee imposed a fine of THB 1,000,000 for this violation.

2. Lack of Appropriate Security Measures

Data controllers are required to implement appropriate security measures, including organizational, technical, and physical measures, in accordance with the minimum standards specified by the PDPC. These measures include:

- Access control for personal data, such as identity verification and proper authorization for access and use of personal data.
- Restricting access to personal data only to authorized employees.
- Regularly reviewing security measures as technology evolves to maintain data security.

In this case, the Committee found that:

1. The data controller did not implement the minimum standard security measures required by law, resulting in personal data violations. Access to customers' personal data was not properly restricted, and almost all employees could access all of the personal data.
2. The data controller lacked **access control measures** for personal data and critical information systems, as well as authorization controls to define access rights. When the company became aware that a large volume of personal data stored in an Excel file had been missing for an extended period, it ignored the issue and failed to improve security measures as required by the PDPA. This negligence led to widespread damage.

The Committee imposed a fine of THB 3,000,000 for this violation.

3. Failure to Report the Breach

Once the data breach occurred, the data controller failed to comply with the PDPA by:

1. Failing to report the breach to the PDPC within 72 hours of becoming aware of the incident. The report should have included details such as the type and nature of the breach, its potential impact, and any remedial measures taken.
2. Failing to notify affected data subjects about the breach and the measures being taken to mitigate its impact, despite the high risk to the rights and freedoms of the data subjects.

For these violations, the Committee imposed a fine of THB 3,000,000.

TMI's Notes

TMI emphasizes that all data controllers should carefully review the PDPA and assess whether their practices fully comply with the law. This first case provides a valuable lesson for all data controllers to thoroughly understand what mistakes can lead to violations and significant fines. It also highlights that the PDPC is rigorous in investigating cases and complaints, serving as a warning to all data controllers to act promptly and proactively to prevent administrative fines or other PDPA violations.

Daiki Koso, Partner
Monchai Varatthan, Partner
Shota Sugiura, Associate
Marin Viriyapongpanich, Paralegal
TMI Associates (Thailand) Co., Ltd.


** This Article is for general informational purposes only and does not constitute legal or tax professional advice. Readers are urged to thoroughly review the information before acting upon it. TMI accepts no responsibility whatsoever with respect to the use of this information.*



 bangkok@tmi.gr.jp

TOKYO | NAGOYA | KOBE | OSAKA | KYOTO | FUKUOKA |
SHANGHAI | BEIJING | YANGON | SINGAPORE | BANGKOK | HA NOI
HO CHI MINH CITY | PHNOM PENH | SILICON VALLEY | LONDON

 Sathorn Square Office Tower, 26th
Floor, unit 2608-2609, North
Sathorn Rd., Silom, Bangrak,
Bangkok 10500

 Facebook: TMI Associates – Thailand
Instagram: tmibkk
LinkedIn: TMI Associates (Thailand)