Global Data and Cyber Handbook - Thailand

Regulators, Enforcement Priorities and Penalties

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# Who are the main data privacy, non-personal data and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: January 2025*

The Personal Data Protection Committee (PDPC)

The Official Information Commission

The Credit Information Protection Committee (CIPC)

The National Cyber Security Committee (NCSC)

The Cybersecurity Regulating Committee (CRC)

# How active is each of the regulator(s)?

*Last review date: January 2025*

☒ Moderately active

As an overview, the main data privacy regulators are the most active compared to other regulators listed in the Thailand chapter of the Handbook. The PDPC is the most active regulator, issuing sub-regulations and interpretative opinions on compliance with the PDPA and its sub-regulations. It has also issued administrative orders against business operators and cooperated with other competent authorities in arresting several individuals who violated the PDPA and other relevant legislation. Both the NCSC and CRC have regularly issued sub-regulations to clarify details, issued warnings, and requested cooperation for compliance with the Cybersecurity Act B.E. 2562 (2019). The Official Information Commission has been active in organizing conferences and discussion seminars, while the CIPC has not been quite active compared to other regulators in these aspects.

# What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last review date: January 2025*

The PDPC has drafted the national data protection promotion and safeguarding plan for Thailand for the years 2024 – 2027. Strengthening law enforcement and promoting data protection awareness are key parts of this plan. Specifically for 2025, the PDPC has revealed that its focus will be on training senior executives, issuing a data protection standard mark (i.e., a Trust Mark), developing a DPO training course, expanding service/complaint centers, and other related areas.

The cybersecurity framework for 2022-2027 aims to efficiently prevent and mitigate cyber threats through stricter enforcement of laws and elevated cybersecurity measures. The Secretary-General of the NCSA stated that the NCSA aims to be a leader in driving Thailand’s cybersecurity efforts. The NCSC’s strategic plan focuses on enhancing defense and response capabilities, raising awareness, and developing high-performing organizations rather than imposing enforcement. Additionally, they operate both reactively and proactively to assist the public in case of damage and to monitor and close vulnerabilities to prevent threats before they occur.

# What trends are you seeing in regulatory investigations relating to data & cyber?

*Last review date: January 2025*

Regulatory investigations or direct enforcement activity by data or cyber regulators are:

☒   Increasing

From a data protection perspective, considering the PDPC’s current priority to achieve zero data leakage, it is anticipated that the PDPC will continue to actively investigate and enforce the PDPA against business operators that violate or fail to comply with the PDPA, particularly in incidents related to data breaches.

☒   Rare

Under the PDPA and the Cybersecurity Act, a class action lawsuit is possible for civil liabilities arising from a breach of the law. However, we have not yet seen an official class action court decision in the data and cyber area.

# What are the potential penalties/remedies for non-compliance with the key data and cybersecurity laws in the jurisdiction?

*Last review date: January 2025*

**There are:**

☒        administrative remedies from regulators and law enforcement

Non-compliance could be punished with administrative fines up to THB 5,000,000 (approximately USD 144,500).

☒        criminal penalties from regulators and law enforcement

Non-compliance could be punished with imprisonment for up to one year, or a fine not exceeding THB 1,000,000 (approximately USD 28,900), or both.

☒        private remedies

The data subject may, for example,

file complaints with the Expert Committee, and

claim compensation for any damage caused to data subjects as a result of operations involving their personal data

The court shall have the power to order the personal data controller or the personal data processor to pay punitive damages of up to twice the actual compensation.

# If data subjects have private remedies, what form can these remedies take?

*Last review date: January 2025*

☒        individual personal actions
☒        class actions

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.