

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2025

Definitive global law guides offering
comparative analysis from top-ranked lawyers

**Thailand: Law & Practice
and Trends & Developments**

Pranat Laohapairoj, Suphakorn Chueabunchai
and Pitchaya Roongroajsataporn
Chandler Mori Hamada



THAILAND



Law and Practice

Contributed by:

Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn
Chandler Mori Hamada

Contents

1. Legal and Regulatory Framework p.4

- 1.1 Overview of Data and Privacy-Related Laws p.4
- 1.2 Regulators p.5
- 1.3 Enforcement Proceedings and Fines p.5
- 1.4 Data Protection Fines in Practice p.6
- 1.5 AI Regulation p.6
- 1.6 Interplay Between AI and Data Protection Regulations p.6

2. Privacy Litigation p.6

- 2.1 General Overview p.6
- 2.2 Recent Case Law p.7
- 2.3 Collective Redress Mechanisms p.7

3. Data Regulation on IoT Providers, Data Holders and Data Processing Services p.7

- 3.1 Objectives and Scope of Data Regulation p.7
- 3.2 Interaction of Data Regulation and Data Protection p.8
- 3.3 Rights and Obligations Under Applicable Data Regulation p.8
- 3.4 Regulators and Enforcement p.8

4. Sectoral Issues p.8

- 4.1 Use of Cookies p.8
- 4.2 Personalised Advertising and Other Online Marketing Practices p.9
- 4.3 Employment Privacy Law p.9
- 4.4 Transfer of Personal Data in Asset Deals p.9

5. International Considerations p.10

- 5.1 Restrictions on International Data Transfers p.10
- 5.2 Government Notifications and Approvals p.10
- 5.3 Data Localisation Requirements p.10
- 5.4 Blocking Statutes p.11
- 5.5 Recent Developments p.11

Contributed by: Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn, Chandler Mori Hamada

Chandler Mori Hamada combines an international standard of practising law with decades of local experience in the Thai legal environment. The firm's team of more than 100 lawyers in Thailand is internationally recognised for its legal expertise in antitrust and competition, aviation, banking and project financing, capital

markets, corporate and mergers and acquisitions, data privacy and data protection, dispute resolution, energy, natural resources and infrastructure, insurance, labour and employment, real estate, REITs, regulatory and public policy, restructuring and insolvency, and technology, media and telecommunications.

Authors



Pranat Laohapairoj is a partner at Chandler Mori Hamada. He has worked with Thai and international clients on mergers and acquisitions, and in the areas of antitrust and

competition, corporate, anti-corruption, compliance, data privacy and data protection, providing advice and services involving due diligence (for mergers and acquisitions, antitrust and data protection), deal structuring, negotiation, contract drafting, deal execution, in-house training and public seminars (for anti-bribery, antitrust and data protection), internal misconduct investigations and antitrust defence. Pranat regularly works on both domestic Thai deals and cross-border investments, and his experience spans multiple sectors.



Suphakorn Chueabunchai is a senior associate at Chandler Mori Hamada and has been with the firm since 2013. He is a specialist in corporate law and has advised clients on mergers

and acquisitions as well as due diligence on Thai target companies. Suphakorn's experience spans multiple sectors, including e-commerce, technology, automotive, tourism, transportation and the import of hazardous substances. He also provides legal advice on foreign investment laws and taxation.



Pitchaya Roongroajsataporn is an associate at Chandler Mori Hamada and a member of the corporate and mergers and acquisitions practice group. She has a particular focus on the

technology, media and telecommunications (TMT) sector, including data protection. Pitchaya's experience includes advising on a broad range of data protection issues including in relation to the PDPA in Thailand, applying for digital asset business licences and providing regulatory advice related to the technology sector.

Contributed by: Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongrojaisataporn,
Chandler Mori Hamada

Chandler Mori Hamada Limited

17th and 36th Floors
Sathorn Square Office Tower
98 North Sathorn Road
Silom
Bangrak
Bangkok 10500
Thailand

Tel: +662 009 5000
Fax: +662 009 5080
Email: business-development@morihamada.com
Web: www.chandler.morihamada.com

CHANDLER MORI HAMADA

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

The Personal Data Protection Act BE 2562 (2019) (PDPA) is the primary law regulating the processing of personal data in Thailand. Similar to other jurisdictions, “personal data” in Thailand is defined as any data that, by itself or in combination with other data, can be traced back to an individual, excluding the data of deceased persons.

The PDPA focuses on the protection of data subjects whose personal data is processed – including by collection, storage, use, disclosure, etc – regardless of the original source of such personal data. Entities that make decisions and process personal data (known as “Personal Data Controllers” or “controllers” under the PDPA) are required to have a lawful basis for processing any personal data and to maintain proper security measures to prevent any loss, unauthorised access, use or disclosure of personal data. These requirements also apply to

service providers who process personal data as instructed by or on behalf of a controller (known as “Personal Data Processors” or “processors” under the PDPA).

The PDPA, which is mainly based on the General Data Protection Regulation (GDPR) of the European Union (EU), has created obligations on the private sector and government (ie, both Personal Data Controllers and Personal Data Processors) regardless of the mode of processing (ie, both automated and non-automated processing), especially regarding burden of proof.

The PDPA itself applies to most activities, with certain exemptions such as:

- household activities;
- the operation of public authority for public safety; and
- media and fine arts activities that are in accordance with professional ethics.

For businesses regulated by specific supervisory authorities (such as banks and insurance businesses), the PDPA allows those supervisory

Contributed by: Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongrojatsaporn,
Chandler Mori Hamada

authorities to issue the standard form or guideline for their operators to follow.

1.2 Regulators

The Personal Data Protection Committee (PDPC) is a supervising authority under the PDPA, while the PDPA established the Office of the PDPC to support the PDPC in developing and facilitating enforcement. Under the PDPA, the PDPC shall have several duties, such as:

- providing a master plan of operation for the promotion and protection of personal data;
- promoting and supporting government agencies and private sectors in order to conduct evaluation of the operational results of such master plan;
- determining measures or guidelines of the operation in relation to data protection, in order to comply with the PDPA;
- issuing notifications or rules for the execution of the PDPA; and
- providing advice or consultancy for any persons.

In addition, the PDPC shall appoint expert committees to consider any complaints under the PDPA, including investigating any act in connection with personal data, settling disputes and carrying out any act assigned by the PDPC.

1.3 Enforcement Proceedings and Fines

As mentioned in **1.2 Regulators**, the expert committee will consider and investigate any complaints on behalf of the PDPC in accordance with the PDPC's rules. If any complaint does not comply with such rules, the expert committee shall not accept such complaint for consideration.

If the expert committee's consideration or investigation finds that such complaint can be settled,

and if the relevant parties are willing to settle, the expert committee must proceed with the dispute settlement before issuance of any order mandating the operator (either the controller or processor) to perform or rectify their act, or prohibiting the operator from carrying out an act that would cause damage to the data subject.

If the operator does not then comply with the expert committee's order, the administrative procedure will be applied (including the power to order seizure, attachment and sale by auction as allowed by law). The expert committee's order shall be final. Any party may appeal such order in accordance with the administrative procedure within 15 days after receiving such order.

In this regard, a PDPC Notification on Administrative Penalties relates to the enforcement of administrative penalties and sets out the criteria for how administrative penalties (as determined by the expert committee) are used. The expert committee will consider and apply administrative penalties to a controller or processor based on the level of seriousness of such offence. Offences are separated into two groups: serious and non-serious offences. Under the Notification on Administrative Penalties, the expert committee is empowered to levy administrative penalties as follows.

Serious Offences

The expert committee can impose administrative fines on a controller and/or processor. In addition, administrative fines can be imposed on offenders who fail to comply with an order from the expert committee to remedy a violation. Such orders include remedying, stopping, suspending or seizing related processing activities.

Contributed by: Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn, Chandler Mori Hamada

Non-Serious Offences

The expert committee may issue orders to remedy, stop, suspend or seize related processing activities, or it may carry out any other acts to stop/minimise the damage within a specific time.

1.4 Data Protection Fines in Practice

On 21 August 2024, the expert committee issued a maximum administrative fine of THB7 million to a major online retail company in Thailand for failing to protect personal data, as required by the PDPA. The company had collected data from over 100,000 customers but did not appoint a data protection officer (DPO) or implement adequate security measures, leading to data leaks to call centre scams. Additionally, the company failed to report the data breach promptly, violating several provisions of the PDPA. The expert committee ordered the company to improve its security measures, arrange for staff training and report all remedy measures back to the Office of the PDPC. This case marks the first major administrative fine imposed under the PDPA, highlighting the government's commitment to enforcing data protection laws and enhancing public trust in online transactions and government projects that require personal data for identity verification.

1.5 AI Regulation

Thailand has introduced the Draft Royal Decree on Business Operations that Use Artificial Intelligence Systems (the "Draft Royal Decree"), influenced by the EU AI Act, for public hearings in 2022 to regulate AI based on risk levels. The Draft Royal Decree mandates that providers of high-risk AI systems implement various measures, such as a risk management system, data governance, record-keeping and cybersecurity measures. Apart from the controlling side, Thailand has also introduced the Draft Act on Promotion and Support for Artificial Intelligence

to enhance AI development through regulatory sandboxes and support from relevant authorities. These draft regulations aim to build trust in AI systems along with ensuring the protection of personal data by enforcing stringent data protection measures and compliance requirements. Unfortunately, since these drafts are still under development by the responsible authorities, the current safeguards for the protection of personal data in the context of AI systems will be governed by the provisions of the PDPA. This existing legal framework will continue to protect personal data until the AI-specific regulations are finalised and enacted, thereby ensuring a seamless transition to more specialised AI data protection standards.

1.6 Interplay Between AI and Data Protection Regulations

Implementation of the primary concept of AI regulation in Thailand derived from the Draft Royal Decree, as mentioned in 1.5 AI Regulation, will significantly impact data protection in relation to AI systems by imposing strict requirements on AI system providers to ensure data security and transparency. The regulations will mandate comprehensive data governance and risk management practices, aligning with the PDPA to safeguard personal data. The authors believe that the regulations will complement the PDPA in the future to ensure that AI systems will be developed and deployed responsibly while protecting individuals' data privacy.

2. Privacy Litigation

2.1 General Overview

As described in 1.3 Enforcement Proceedings and Fines, the PDPA provides the expert committee with an enforcement power to issue an administrative order for addressing any mis-

Contributed by: Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn, Chandler Mori Hamada

conduct under the PDPA. However, most cases have been discharged or have ceased at the expert committee stage, and there are no court cases regarding personal data that are publicly available in Thailand.

In addition to the powers of the expert committee, the PDPA covers three types of liabilities:

- criminal liabilities;
- administrative liabilities; and
- civil liabilities.

For criminal liabilities, the authority may pursue a criminal case against any commercial operator who has breached the PDPA. Any use or disclosure of sensitive data without consent, and which has caused damage to the data subject, carries penalties of imprisonment of up to six months, a fine of up to THB500,000 or both. However, any use or disclosure, if undertaken for undue benefit of the commercial operator, will double the above-stated maximum imprisonment duration and fine amount. In this regard, the relevant director or manager of the juristic person may be subject to the same penalties as the juristic person.

As described in **1.3 Enforcement Proceedings and Fines**, the PDPC Notification on Administrative Penalties governs the enforcement and criteria relating to administrative liabilities.

For civil liabilities, a damaged data subject may bring a civil suit against a controller and/or processor who has wronged them. The PDPA expressly allows the court to award punitive damages, which is generally rare in Thailand, and such damages shall not exceed two times the actual damages (if the court believes the breach is severe). As this civil liability is based on tort law and privacy cases often involve more

than one impacted data subject, class actions are allowed for privacy cases.

2.2 Recent Case Law

As described in **1.3 Enforcement Proceedings and Fines** and **2.1 General Overview**, there have been no significant litigation cases in privacy or data protection law in Thailand, as most cases tend to be resolved at the expert committee level.

2.3 Collective Redress Mechanisms

In Thailand, the concept of collective redress exists within the legal framework, commonly referred to as a “class action”. However, its application and procedures remain limited and are still evolving. Victims of data protection violations are entitled to file a case against offenders through the class action mechanism, as data protection breaches typically fall under tort claims. In practice, for high-profile cases (affecting many individuals), the Office of the PDPC often encourages victims to provide their information before initiating an investigation and taking appropriate action.

3. Data Regulation on IoT Providers, Data Holders and Data Processing Services

3.1 Objectives and Scope of Data Regulation

There are no specific regulations concerning the use of internet of things (IoT) services in Thailand. The providers of IoT services shall be deemed as controllers or processors under the PDPA, depending on whether such service providers are determining the processing activities and fall under the provisions of the PDPA. The role obligations are as follows.

Contributed by: Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn, Chandler Mori Hamada

Controllers

Controllers must:

- provide appropriate security measures for preventing the unauthorised or unlawful loss, access to, use, alteration, correction or disclosure of personal data;
- in a circumstance where personal data is disclosed to other persons, take action to prevent such person from using or disclosing such personal data unlawfully or without authorisation;
- establish a system to erase or destroy personal data when the retention period ends, the data becomes irrelevant or is beyond the purpose for which it has been collected or the data subject puts in a request or withdraws consent, except when the data is needed in relation to freedom of expression, legal claims or compliance with the law; and
- notify the Office of the PDPC of any personal data breach.

Processors

Processors must:

- carry out the processing of personal data only pursuant to the instruction given by the controllers, except where such instruction violates any laws or any provisions in the PDPA;
- provide appropriate security measures for preventing unauthorised or unlawful loss, access to, use, alteration, correction or disclosure of personal data; and
- notify the controller of personal data breaches.

3.2 Interaction of Data Regulation and Data Protection

As mentioned in **3.1 Objectives and Scope of Data Regulation**, there are no specific regula-

tions concerning the use of IoT services or data processing services in Thailand; only general PDPA provisions shall be applied.

3.3 Rights and Obligations Under Applicable Data Regulation

Concerning rights and obligations under applicable data regulation, please see **3.1 Objectives and Scope of Data Regulation**.

3.4 Regulators and Enforcement

Concerning regulators and enforcement, please see **1.2 Regulators** and **1.3 Enforcement Proceedings and Fines**.

4. Sectoral Issues

4.1 Use of Cookies

Currently, there is no specific legislation in Thailand that regulates the use of cookies, but as the use of cookies is considered to fall under the processing of personal data, it shall also fall under the principles of the PDPA as follows:

- strictly necessary cookies or essential cookies are required for the basic functioning of a website, and explicit consent is not required as they can be used on a contractual basis;
- performance and functional cookies are used to enhance user experience and improve website performance, and explicit consent from users is required prior to the use of such cookies; and
- targeting and advertising cookies track user behaviour for personalised advertising and are not necessary for any functions on the website, so explicit consent for their use is required.

Concerning the general requirements for using any type of cookie, the PDPA requires controllers

Contributed by: Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn,
Chandler Mori Hamada

to provide clear information about the purpose and function of each type of cookie, typically through a cookie, policy and cookie, banners or pop-ups that are designed to inform users and obtain their consent. The details therein shall be similar to other notifications for data processing provided to data subjects, namely the types of cookies used on the website, the personal data to be processed, the purposes of processing, the retention period, the rights of data subjects, etc. In addition, users must have the ability to manage their cookie, preferences, withdraw consent, and access or delete data collected through cookies.

4.2 Personalised Advertising and Other Online Marketing Practices

Generally, online marketing may be based on legitimate interest or consent of the data subject. Personalised advertising is regarded as too intrusive for data subjects, and consent under the PDPA is therefore required.

In addition to the PDPA, online marketing may be classified as computer data or electronic mail under the Computer-Related Crime Act BE 2550 (2007). Where an operator sends any computer data or electronic data (such as via email, short message service (SMS) or comments) to another person in a manner that disturbs that person, such operator must give that person an easy opportunity to cancel or provide notification of their wish to deny receipt of such computer data or electronic mail (ie, an opt-out option). Otherwise, such operator shall be liable to a fine not exceeding THB2 million. Once any person requests cessation, the operator must stop sending such marketing messages immediately (ie, after no more than seven days).

4.3 Employment Privacy Law

Similar to other relationships, the enactment of the PDPA has significantly impacted the employment relationship, particularly in terms of how employers collect, use and manage employees' personal data. The PDPA requires employers to obtain specific consent from employees before collecting their personal data, including sensitive personal data, ensuring transparency from recruitment through the entire employment life cycle.

The PDPA emphasises data minimisation and purpose limitation, requiring employers to collect only the personal data necessary for specific purposes related to employment – eg, to fulfil the employment process, provide employee benefits or manage payroll. Employers must ensure that personal data is used solely for the purposes for which it was collected and in accordance with the employees' privacy policy. In addition, employers also have the obligations to maintain data security and comply with other provisions regarding the controllers' obligations under the PDPA (for more details, please see **3.1 Objectives and Scope of Data Regulation**).

As data subjects, employees are granted several rights under the PDPA, such as the right to access, correct and delete their personal data and the right to withdraw consent for data processing, among others. Employers must establish procedures to facilitate these rights, allowing employees to control their personal data, thereby enhancing privacy and trust in the employer-employee relationship.

4.4 Transfer of Personal Data in Asset Deals

There are no specific regulations concerning the transfer of personal data in asset deals in Thai-

Contributed by: Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn, Chandler Mori Hamada

land. Only general PDPA provisions are applicable to this area.

5. International Considerations

5.1 Restrictions on International Data Transfers

The PDPA does not provide for the concept of absolute restriction for any type of transfer of personal data outside the jurisdiction of Thailand. Instead, controllers, as the transferors, may be subject to several obligations and/or must ensure that the transferee meets the qualifications as prescribed under the PDPA.

In general, in the case of transfer of personal data outside Thailand, the countries in which the transferee is located should have adequate personal data protection measures. The list of countries deemed to have adequate personal data protection measures is set to be prescribed by the PDPC; however, such list has not yet been prescribed. Two key criteria to consider in determining whether a country has adequate personal data protection measures are as follows:

- whether the legal safeguards for personal data protection in such country are of the same standard as or higher than those under the PDPA; and
- whether such country has a proper authority or organisation for enforcing the above-mentioned safeguards.

In any event, even upon the prescription of such list, several exemptions exist where the controller may transfer the personal data to countries not on the list (regarding compliance with the law, obtaining consent from the data subject, the execution of a contract to which the data subject is one of the parties, etc).

Another exemption to the limitation of personal data transfer to only those countries included on the list applies when the following qualifications are fulfilled:

- where such transfer is within a group of undertakings or enterprises; and
- where the transferor of the personal data applies the binding corporate rules (BCRs), which have already been approved by the PDPC office, to such transfer.

During the period when no list is prescribed for those countries deemed to have adequate personal data protection, or when the BCRs have not been approved by the PDPC office, the PDPA stipulates that the transferor provide appropriate security measures, to be enacted in accordance with the rights of the data subject, as well as effective legal remedial measures such as appropriate standard contractual clauses (SCCs) for cross-border transfer and a certificate. Under the PDPA's notification, SCCs from the Association of Southeast Asian Nations (ASEAN) Model Contractual Clauses for Cross-Border Data Flows and GDPR SCCs are acceptable.

5.2 Government Notifications and Approvals

Cross-border transfer does not require government notification or approval.

5.3 Data Localisation Requirements

In certain cases, operators have to retain documents on their premises, such as accounting documents and a VAT certificate. However, an operator can duplicate and transfer such data internationally (see 5.1 Restrictions on International Data Transfers for more details).

Contributed by: Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn, Chandler Mori Hamada

5.4 Blocking Statutes

There are no blocking statutes under Thai privacy laws.

5.5 Recent Developments

On 25 December 2023, the PDPC introduced two notifications regarding cross-border transfers of personal data under Sections 28 and 29, with the details summarised as follows.

Notification Regarding Criteria for Adequate Countries (Section 28)

This notification outlines two key criteria for determining if a destination country qualifies as having adequate data protection standards:

- the legal system pertaining to personal data protection in the destination country must be at least equivalent to or more stringent than the PDPA; and
- the country must have a proper authority or organisation to enforce its data protection laws.

In any case, the transferor is entitled to assess the adequacy of the destination country's data protection standard by itself. Additionally, the PDPC may consider and issue a list of adequate countries in the near future.

Notification Regarding Appropriate Safeguards (Section 29)

In the absence of an "adequacy list", cross-border transfers can only occur if data exporters implement appropriate safeguards to ensure PDPA-compliant protection standards. This notification sets out types of and criteria for certain acceptable safeguards under the PDPA, which shall include BCRs, SCCs and certifications.

- BCRs are legally binding data protection policies adhered to by related parties, including related groups or affiliated companies, for cross-border data transfers. In any case, the parties to the transfer must obtain PDPC approval prior to the application of BCRs.
- SCCs are standardised data protection provisions that ensure compliance with data protection laws. They must address data processing activities and legal compliance, regulating controllers and processors to maintain data security standards. This notification allows the parties involved in data transfer to refer to SCCs from certain international models, including those of the EU and ASEAN.
- Controllers or processors may consider obtaining a certification for their cross-border data transfer and related processing activities; the details are subject to further announcement.

Trends and Developments

Contributed by:

Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn
Chandler Mori Hamada

Chandler Mori Hamada combines an international standard of practising law with decades of local experience in the Thai legal environment. The firm's team of more than 100 lawyers in Thailand is internationally recognised for its legal expertise in antitrust and competition, aviation, banking and project financing, capital

markets, corporate and mergers and acquisitions, data privacy and data protection, dispute resolution, energy, natural resources and infrastructure, insurance, labour and employment, real estate, REITs, regulatory and public policy, restructuring and insolvency, and technology, media and telecommunications.

Authors



Pranat Laohapairoj is a partner at Chandler Mori Hamada. He has worked with Thai and international clients on mergers and acquisitions, and in the areas of antitrust and

competition, corporate, anti-corruption, compliance, data privacy and data protection, providing advice and services involving due diligence (for mergers and acquisitions, antitrust and data protection), deal structuring, negotiation, contract drafting, deal execution, in-house training and public seminars (for anti-bribery, antitrust and data protection), internal misconduct investigations and antitrust defence. Pranat regularly works on both domestic Thai deals and cross-border investments, and his experience spans multiple sectors.



Suphakorn Chueabunchai is a senior associate at Chandler Mori Hamada and has been with the firm since 2013. He is a specialist in corporate law and has advised clients on mergers

and acquisitions as well as due diligence on Thai target companies. Suphakorn's experience spans multiple sectors, including e-commerce, technology, automotive, tourism, transportation and the import of hazardous substances. He also provides legal advice on foreign investment laws and taxation.



Pitchaya Roongroajsataporn is an associate at Chandler Mori Hamada and a member of the corporate and mergers and acquisitions practice group. She has a particular focus on the

technology, media and telecommunications (TMT) sector, including data protection. Pitchaya's experience includes advising on a broad range of data protection issues including in relation to the PDPA in Thailand, applying for digital asset business licences and providing regulatory advice related to the technology sector.

Contributed by: Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongrojaisataporn,
Chandler Mori Hamada

Chandler Mori Hamada Limited

17th and 36th Floors
Sathorn Square Office Tower
98 North Sathorn Road
Silom
Bangrak
Bangkok 10500
Thailand

Tel: +662 009 5000
Fax: +662 009 5080
Email: business-development@morihamada.com
Web: www.chandler.morihamada.com

CHANDLER
MORI HAMADA

Move Towards Compliance – Data Protection, Privacy Compliance and Action Trends in Thailand

Data protection

The Personal Data Protection Act B.E. 2562 (2019) (PDPA) was introduced over five years ago and has become a cornerstone regulation in Thailand. While initially heralded as a new legal framework, both in terms of its enactment and the introduction of data protection concepts unfamiliar to many in Thailand, its enforcement has significantly intensified in recent years. Data protection and privacy, which were relatively niche topics at the time of the PDPA's enactment, are now essential concerns for businesses and individuals alike. Prior to the PDPA, personal data in Thailand was often mined, collected, stored, sold, transferred, analysed, and used – often without the consent of the data subjects. The absence of a comprehensive legal framework meant that such practices were largely unregulated, and general tort law provided little recourse for those affected, given the difficulty of proving damages and the lack of deterrence against non-consensual data use. This created an environment where many businesses prioritised economic gains over ethical data practices,

leveraging personal data with minimal concern for legal repercussions.

However, this landscape has shifted dramatically with the PDPA's introduction and the growing focus on enforcement. Over the past five years, medium-sized and large companies – particularly those affiliated with global corporations or operating in jurisdictions with stringent data protection laws – have steadily implemented measures to comply with the PDPA. This compliance trend has gradually influenced smaller and local businesses, though adoption has been slower among some small and medium-sized enterprises. Despite the time that has passed, there remain organisations that are only beginning their compliance journey. The increasing enforcement of the PDPA serves as a critical reminder that adherence to data protection standards is no longer optional but an essential aspect of operating within Thailand's modern regulatory framework.

Compliance

Over three years since the full enforcement of the PDPA, many operators in Thailand have taken significant steps to ensure compliance

Contributed by: Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn,
Chandler Mori Hamada

through comprehensive audits and evaluations of their data protection frameworks. The authors have observed a clear and consistent trend toward stricter compliance and increased efforts to address the requirements of the PDPA. For instance, numerous companies, especially medium-sized and large organisations, have conducted PDPA compliance audits to assess and enhance the effectiveness of their existing frameworks. These companies have invested substantial resources into data analysis, due diligence, and mapping exercises, including conducting structured personnel interviews across various business units. Such interviews, particularly those targeting departments heavily involved in personal data handling (eg, human resources, sales, administration, and IT), have proven to be highly effective. When correctly implemented using ethnographic methods, these interviews provide comprehensive insights into:

- specific personal data items being used;
- the rationale for their use;
- timing and processes for collection, use, and storage;
- data transfer practices; and
- data deletion or destruction processes.

These interviews also serve a dual purpose by inadvertently providing training for both interviewees and internal data protection teams. Issues identified during the process often lead to discussions of legal principles and rationale, enhancing overall awareness of the PDPA. The insights gathered allow companies to create precise and tailored documentation, such as policies, consent forms, protocols, and impact assessments, addressing specific data protection needs.

Companies often discover risks associated with their data utilisation processes during these audits. Many have realised that high-risk processes previously considered acceptable must now be terminated, while others can be justified and retained with proper documentation under the PDPA framework. While interviews remain a robust method for gathering detailed data, some companies have opted for a more economical approach using questionnaires. Custom questionnaires are distributed to key business units to collect data on utilisation processes, including points of collection, storage locations, access limitations, transfers, and deletion. While this method is quicker and less expensive than interviews, it tends to produce less detailed results, thereby increasing the likelihood of oversight. Companies relying solely on questionnaires often struggle to notify data subjects comprehensively or obtain appropriate consent, leading to gaps in compliance.

Notably, many businesses initially favoured questionnaires as a “quick fix”, given the incomplete supplemental rules under the PDPA. However, some later realised that the resulting PDPA documentation lacked the necessary depth and specificity, prompting them to undertake more thorough interviews – a costly and time-intensive process in hindsight. Smaller companies, often constrained by budgetary concerns, have adopted even simpler approaches, such as using off-the-shelf templates with minimal customisation. While this strategy requires less time and financial investment, it carries significant risks. Generic templates often fail to capture the unique data utilisation processes of an organisation, leaving gaps that heighten the likelihood of legal breaches, such as inadequate notifications or consent failures. Consequently, this method is generally discouraged.

Contributed by: Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn, Chandler Mori Hamada

In conclusion, as the PDPA enters its third year of full enforcement, it is evident that compliance efforts have become more widespread and sophisticated. Many operators are now focusing on fine-tuning their PDPA frameworks to ensure ongoing compliance and mitigate risks effectively. However, for organisations that have yet to prioritise comprehensive audits or proper compliance measures, the growing enforcement environment underscores the urgency of adopting robust data protection practices.

Action trends

One positive note on the compliance action trend in Thailand is that regardless of what internal due diligence methodology is used (whether in-depth and detailed personnel interviews, quick questionnaires, or template customisation based purely on limited existing knowledge), many companies in Thailand have come up with data protection and privacy documents that are required by law. Some versions and forms are naturally more complete and more compliant than others, and some are more detailed due to larger amounts of information elicited from fact-finding processes; overall, though, these companies have done reasonably well in terms of moving in alignment with the law. Basic documents that have been seen include:

- data protection and privacy policies;
- consent forms;
- cookie-collection mechanisms;
- data protection officer appointment announcements;
- data processing agreements or data protection clauses with counterparty;
- specific protocols and standards of operation; and
- complaint reports.

Another positive note on the compliance action trend in Thailand is the surge in data breach reports. The PDPA requires an entity to notify the PDPC of a known or discovered data breach that may have an impact on data owners, whether from accidental leakage (unintended transfer, loss of electronic storage device, system failure leading to loss or corruption of data, etc) or from intentional acts (unlawful access from hacking, phishing, ransomware, etc) within 72 hours of becoming aware of such incident. So far, hundreds of cases have been reported to the PDPC since the PDPA's inception – many more than most anticipated. This surge in incident reports signifies two things.

First, it shows a worrying trend of a rise in electronic crime related to personal data, not just in Thailand but globally. In fact, most cases that have been filed with the PDPC in Thailand pursuant to the PDPA were the results of offshore breaches or hacking activities that had nothing to do with Thailand, but filing had to be undertaken in Thailand as Thai citizens and residents were affected by such offshore incidents.

Second, it shows a positive trend of self-learning and self-imposed compliance. Although there may be little communication between the PDPC and other data protection regulators from other countries (meaning that awareness of an incident in one jurisdiction is unlikely to be communicated to another jurisdiction), these local companies (whether subsidiaries of international corporations or otherwise) have chosen to voluntarily comply with the legal requirements and to report their accidental failures, despite the risk of discovery being small.

Part of this surge in willingness to comply with the requirements of the PDPA is due to the fact that the PDPC has provided fair and reasonable

Contributed by: Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongroajsataporn, Chandler Mori Hamada

judgments in past cases. Before mid-2024, no company had been fined for late reporting of a breach incident, although statistically speaking most companies report long after 72 hours from discovery, simply because it normally takes many days for the companies to become aware of a breach or an attack. Further days or even weeks are needed to analyse and pinpoint whether any person in Thailand has been particularly affected, and if so, whether such impact rises to the level that must be reported to the PDPC. It may also take a few more days for the companies to consult with external experts on what to do. However, it appears that the PDPC has recently adopted a stricter stance on late notifications. To date, the PDPC seems to be increasingly focused on the supporting reasons behind such delays, to the extent that a company has already been fined for delayed reporting data breach, placing greater emphasis on the diligence and timeliness of companies in addressing breach incidents.

Previously, the PDPC has been very understanding. As long as a report is filed properly and expediently (to the extent possible), questions from the PDPC are satisfactorily answered when asked, and the report-makers do not act unreasonably or tardily, the PDPC will show leniency. This, however, is because the PDPC would like to allow operators in Thailand to understand the law and to have enough time to adjust well to the legal requirements, whether on internal training of employees regarding understanding and avoiding risks, or on the documentation side. Nowadays, following the full implementation of the PDPA and the issuance of a number of subordinate regulations, the PDPC has adopted a more proactive approach to enforcement. When cases are reported, the PDPC promptly initiates some actions including investigating the case, ordering companies to provide clarifications, or

co-ordinating with relevant authorities to undertake necessary actions. Notably, the PDPC has established the “PDPC Eagle Eye” to specifically address data breach incidents. This complaint centre not only focuses on investigating and responding to breaches but also aims to educate and alert the public, monitor compliance, and manage complaints effectively.

Moreover, in 2024, Thailand witnessed its first penalty case under the PDPA. The PDPC imposed a maximum administrative fine of THB7 million on a major online retail company in Thailand for failing to comply with key data protection requirements under the PDPA. These violations included the failure to appoint a Data Protection Officer (DPO) and to implement adequate security measures, which resulted in data leaks that were subsequently exploited in call centre scams. Furthermore, the company failed to report the data breach within the timeframe specified under the PDPA. This landmark case initiates a significant step in demonstrating the government’s commitment to enforcing data protection laws, fostering public trust in online transactions and government initiatives that require personal data for identity verification.

A third positive note is that most companies, especially those belonging to a global operation or those with routine contacts with offshore companies that hail from jurisdictions with relevant data protection and privacy law, have been much more careful regarding transfer of personal data. Most companies have been comparatively more reluctant about such transfer, and this has manifested in discussions during business meetings as well as in execution of documents to cover transfer of data for any particular project. Some companies have even gone so far as to re-train their project personnel on PDPA requirements prior to commencement of each project.

Contributed by: Pranat Laohapairoj, Suphakorn Chueabunchai and Pitchaya Roongrojatsaporn,
Chandler Mori Hamada

This shows that many companies do put extra care into ensuring compliance with the PDPA.

The fourth positive development observed by the authors also carries a layer of complexity. Many ordinary citizens and residents in Thailand have become increasingly vocal about exercising their rights under the PDPA. This shift has brought about both beneficial and problematic outcomes. On the positive side, the heightened awareness and growing likelihood of complaints have compelled businesses to accelerate their compliance efforts. However, this has also led to increased operational costs for many businesses, driven not only by compliance measures but also by the need to handle a surge in complaints and allegations – many of which are ungrounded or stem from misunderstandings of the law. In some cases, the authors have noticed a more concerning trend where individuals may leverage their rights under the PDPA with hidden agendas. For example, certain data subjects use PDPA complaints strategically as a tool to negotiate compensation or settlements under unrelated legal claims, effectively weaponising the rights granted by the law. This misuse poses additional challenges for businesses, as they must navigate both legitimate and opportunistic claims, often at considerable financial and operational expense. While the increased awareness of data protection rights is a positive sign of the PDPA's influence, the potential for misuse underscores the importance of educating both businesses and the public on the proper application and limits of the law.

Summary

Overall, Thailand-based companies are steadily progressing towards compliance with the PDPA. Large multinational companies have taken the lead, setting an example for local entities, which have been gradually following suit. The year 2024 saw the issuance of several supplementary updates aimed at strengthening enforcement, especially for cross-border requirement and DPO appointment. However, 2025 marks a significant milestone as it represents five years since the PDPA's full enforcement, triggering a formal review by the authorities. This review is anticipated to assess the effectiveness of the PDPA, identify gaps in the current framework, and propose amendments or new supplemental regulations to address evolving challenges in data protection and privacy. These potential updates may introduce additional compliance requirements or clarify existing ambiguities, further emphasising the importance of proactive measures by businesses. As enforcement is likely to intensify following the review, companies are strongly encouraged to deepen their understanding of the PDPA and undertake thorough compliance exercises as soon as possible. By doing so, they can minimise – or ideally eliminate – legal and operational risks associated with non-compliance while staying ahead of any forthcoming regulatory changes.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com