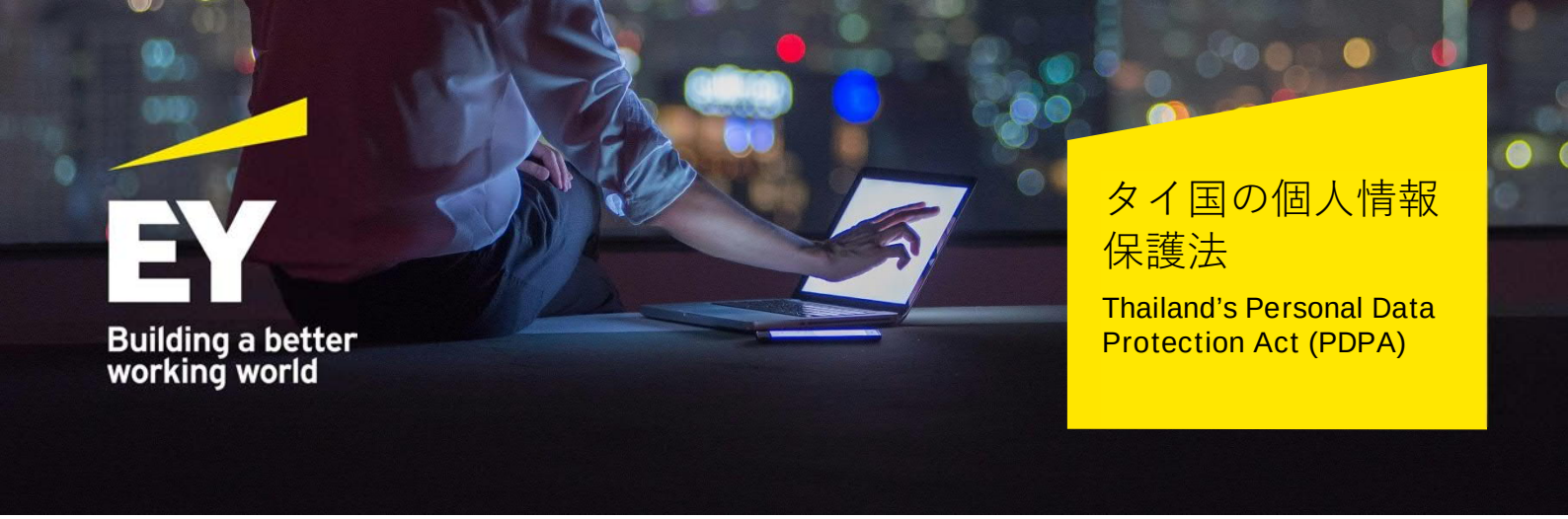

タイ国の個人情報保護法

Thailand's Personal Data Protection Act (PDPA)

仏歴 2562 年（2019）個人情報保護法は 2021 年 6 月 1 日に全面施行されます。

The Personal Data Protection Act B.E. 2562 (2019) will be fully effective on 1 June 2021.

個人情報保護法とは？

個人情報保護法の主たる目的は、個人の個人情報を適切に保護し、

- データ所有者をプライバシーの侵害から保護し、且つ
- 個人情報が悪用された場合に、データ所有者に対する救済措置を確立することです。

この文脈において個人情報は、直接又は間接的に、個人を識別することを可能にする任意のデータです。これは紙、電子フォーマット、テキスト、写真又は音声を含む任意の形式をとることができます。例としては、個人識別番号、人種、医療記録及び監視カメラ記録があります。

What is the purpose of the PDPA?

The main purpose of the Act is to adequately safeguard individuals' personal data in order to:

- Protect data owners from violations of their privacy, and
- Establish relief measures for data owners in the event their personal data is misused.

In this context personal data is any data that allows an individual to be identified, whether directly or indirectly. It can be in any form, including paper, an electronic format, text, photo, or audio. Examples are personal identification number, race, medical history, and CCTV records.

対象となる法人

同法は、個人情報を受け取り、データ管理者又はデータ処理者である私法人及び公法人の両方(並びに個人又は法人)に適用されます。

- データ管理者(data controller)とは、個人情報の収集、利用及び開示に関する意思決定を行う者です。
- データ処理者(data processor)とは、データ管理者(サービスプロバイダー)の命令により、又は代理として、個人情報を収集、利用又は開示する者です。

Applicable entities

The Act applies to both private and public entities (and to individuals or juristic persons) who receive personal data and are Data Controller or Data Processor.

- Data Controller is a person making decisions on the collection, use, and disclosure of personal data
- Data Processor is a person who collects, uses, or discloses personal data by order of or on behalf of a data controller (service provider).

個人情報保護法の順守のために、事業者がとるべき行動は？

事業者は、個人情報の収集、利用又は開示に関する現在の慣行を再検討し、現在の慣行と、個人情報保護法に従い個人情報を保護する目的で必要な措置を実施するための個人情報保護法要件の間のギャップを評価する必要があります。

個人情報保護法を順守するために取られる行動は以下のとおりです（但しこれらに限りません）。

1. 運用プロセス中の「個人情報」(personal data)及び「機密個人情報」(sensitive personal data)の全項目を特定する
2. 全ての個人情報が、適法な基準(lawful basis)に基づいて収集、利用及び開示されることを確認する
3. 個人情報保護ポリシー及び関連手続を作成する
4. 個人情報保護法と整合させるため、同意、契約又は契約条件を再検討し修正（又は作成）する
5. データ主体(data subject)が法律に従ってその権利を行使する際に、ガイダンスとして使用するためにデータ主体リクエスト手続を作成する
6. 個人情報漏洩管理手順を作成する
7. 第三者に対する/国境を越えたデータの転送ポリシー及び手続を作成する
8. 個人情報の処理を外注する場合に使用するポリシー及び手続を作成する
9. デジタル経済社会省（Ministry of Digital Economy and Society）が規定した基準に従って個人情報を保護するための情報セキュリティ対策を再検討、再整理、確立及び改善する
10. プライバシーに関する声明をウェブサイトに掲載する
11. 組織が個人情報保護法順守のために確立した個人情報保護法要件及び手続/措置を確実に理解させるため、全関係人員を研修する

個人情報管理には法人内の全機能が関係し、継続的な活動として実施されます。

What actions do business operators need to take for PDPA compliance?

Business operators are required to revisit current practices of collection, use, or disclosure of personal data, and assess gaps between the current practices and PDPA requirements to implement necessary measures to protect personal data in compliance with the PDPA.

Actions to be taken to comply with the PDPA include (but are not limited to) the following:

1. Identify all items of “personal data” and “sensitive personal data” in the operational processes
2. Ensure that all personal data are collected, used and disclosed under a right lawful basis
3. Prepare a Personal Data Protection Policy and associated procedures
4. Revisit and modify (or prepare) consent, contracts or terms of the agreement to align them with the Act
5. Prepare a Data Subject Request Procedure to use as guidance when a data subject exercises his/her rights according to the Act
6. Prepare a Personal Data Breach Management Procedure
7. Prepare a Third Party / Cross Border Data Transfer Policy and Procedures
8. Prepare a policy and procedure for use when outsourcing the processing of personal data
9. Revisit, rearrange, establish or improve data security measures to safeguard personal data, in line with the standards prescribed by the Ministry of Digital Economy and Society
10. Post a Privacy Statement on the website
11. Train all relevant personnel to ensure they understand PDPA requirements and the procedures/measures the organization has established for PDPA compliance

Personal data management involves all functions in an entity and is a continuous activity.

効果的且つ効率的な個人情報管理は、次の条件に依存します。

- 取締役及び幹部によるガバナンスと全人員の関与
- 個人情報保護施策を組み込んだプロセスの設計
- テクノロジーを使用して、業務、ポリシー違反、確立済みの対策を監視し、外部の脅威を検出して対応する

罰則規定

- 刑事罰：1年以下の禁固又は100万バーツ以下の罰金又はその併科。違反者が法人であるとき、行為を指示又は実行する責任者が、係る行為の指示又実行に関し不作為があった場合に、当該責任者は、法人と同じ規定の下で責任を負うものとする。
- 民事責任：実際の損害額の2倍以下の賠償に加えて、懲罰的損害賠償。
- 行政罰：違反は、500万バーツ以下の罰金で処罰される。

罰則規定の原則と根拠は、欧州連合の一般データ保護規則(General Data Protection Regulation: GDPR)と異なりません。2018年のブリティッシュ・エアウェイズのデータ侵害は、係る罰則がどのように適用されるかの一例です。当該航空会社は、およそ50万人の顧客に影響を与えたデータ侵害に対して2億3000万米ドル(70億バーツ)の罰金に直面しましたが、GDPRに基づく罰金は2,000万ユーロ又は会社の全世界の年間売上高の4%の高い方とされます。タイ国においては科料は500万バーツ以下であり、比較的小さなものです。

但し、被害者が多数いる場合は、事業者は各人に対して補償を行う責任も負います。

個人情報保護法ではまた、違反に応じて、データ管理者による同法違反一件ごとに6ヶ月又は1年の禁固刑を課すことも可能です。

Effective and efficient personal data management depends on the following:

- Governance by directors and executives and the involvement of all personnel
- Design of processes to embed personal data protection measures
- Use of technology to monitor operations, violations of policies and established measures, as well as to detect and respond to external threats

Penalties

- Criminal penalties – Imprisonment of up to 1 year and/or fines of up to Baht 1 million. When the offender is a juristic person, if a person responsible for instructing or performing any act omits to instruct or perform such act, that person shall be liable under the same provision as the juristic person.
- Civil liabilities – Punitive damages in addition to actual compensation of up to 2 times the amount of the actual damages.
- Administrative penalties – Non-compliance could be punished with fines of up to Baht 5 million.

The principles and rationale for penalties do not differ from those of the EU's General Data Protection Regulation (GDPR). The British Airways data breach in 2018 is an example of how such penalties apply. The airline faced a USD 230 million (Baht 7 billion) fine for a data breach affecting roughly 500,000 customers. However, under the GDPR fines are up to the higher of EUR 20 million and 4% of the company's global annual turnover, while in Thailand the maximum administrative fines are relatively small at up to Baht 5 million.

However, if there are a number of injured persons, business operators will be responsible for compensating each person.

The Act also allows for imposition of prison terms of 6 months or 1 year for each violation of the Act by a data controller, depending on the offense.

コンタクト

カモンラット・ヌチットプラシティチャイ
パートナー
オフィス電話: +66 2264 9090
Kamolrat.Nuchitprasitchai@th.ey.com

ペンナパー・プークカラット
パートナー
オフィス電話: +66 2264 9090
Pennapa.Pookkarat@th.ey.com

Contact person

Kamolrat Nuchitprasitchai
Partner
Office: +66 2264 9090
Kamolrat.Nuchitprasitchai@th.ey.com

Pennapa Pookkarat
Partner
Office: +66 2264 9090
Pennapa.Pookkarat@th.ey.com

日本デスク
Japan Business Services

山岡　耕志郎（アソシエイト・パートナー）
Koshiro Yamaoka (Associate Partner)
Tel: +66 2264 9090 ext. 54030
Email: Koshiro.Yamaoka@th.ey.com

江橋　美恵（アソシエイト・パートナー）
Mie Ebashi (Associate Partner)
Tel: +66 2264 9090 ext. 54033
Email: Mie.Ebashi@th.ey.com