岩田合同法律事務所 ニュースレター
2025 年 10 月

グローバル法務

タイ個人データ保護法制の執行状況及び特に留意すべき義務

弁護士 松田 章良 ／ 別府 文弥 ／ 深津 春乃

第1 はじめに

2022 年 6 月 1 日にタイの個人データ保護法（Personal Data Protection Act B.E. 2562。以下「PDPA」といいます。）が全面施行されて 3 年以上が経ちました。施行後最初の 2 年間は、タイ個人データ保護委員会（以下「PDPC」といいます。）は、ガイドラインや研修を提供し PDPA の浸透に注力しておりましたが、2024 年 8 月に初めて PDPA 違反事例に対して罰金を科したことを皮切りに、違反行為のエンフォースメントにも積極的な姿勢をみせるようになりました。2025 年 8 月にも新たに 5 件の罰金事例が公表され、これまで科された罰金の総額は計 6 件で約 2,150 万バーツ（約 1 億円弱[1]）に上っています。
本稿では、PDPA の概要を振り返るとともに、これまでの執行事例をご紹介し、特に留意すべき PDPA 上の義務について解説します。

[1] 1 バーツ＝4.6 円で計算。以下同じ。

© IWATA GODO 2025

第2　PDPA の概要

1　「個人データ」の定義・適用対象者・地理的適用範囲

PDPA の対象である「個人データ」とは、生存する自然人に関する、当該自然人を直接又は間接に特定可能な情報をいいます（PDPA（以下省略）6 条）。

PDPA は、データ管理者（Data Controller）及びデータ処理者（Data Processor）を規制対象としています。データ管理者は個人データを収集、使用及び開示する権限を有する個人又は法人、データ処理者はデータ管理者に代わり、又はその指示に従って、個人データを収集、使用及び開示する個人又は法人をいいます（同条）。

PDPA は、①タイ所在のデータ管理者・データ処理者が個人情報の収集、使用又は開示をする場合に適用があることに加え、②タイ国外所在のデータ管理者・データ処理者であっても、(a)タイのデータ主体に商品・サービスを提供する場合、又は(b)タイ国内におけるデータ主体の行動を監視する場合に適用があります（5 条）。

したがって、日本企業のタイ所在の子会社、支店及び駐在事務所が顧客や従業員の情報を保有する場合に加えて、タイに拠点がない日本企業であっても、タイ所在の顧客向けに商品・サービスを提供する場合や、マーケティング目的などでタイ所在の顧客の行動を追跡する場合などには、PDPA が適用されます。

2　データ管理者・データ処理者の主な義務

データ管理者・データ処理者の主な義務としては、以下のものがあります。最近の違反事例に照らして特に重要な義務について、以下第 4 で詳細に取り上げます。

- 個人データ収集時の同意取得・通知義務（23 条）
- 適切なセキュリティ対策の実施義務（37 条、40 条）
- データ管理者の記録保持義務（39 条）
- データ保護責任者（DPO）の選任義務（41 条）
- 越境移転に関するルール（28 条、29 条）

第3　PDPC の執行状況

PDPC は組織の種類や規模を問わずあらゆる業種で PDPA 違反を取り締まっており、これまで 6 件の違反事例について行政罰を科しています。具体的なケースは以下のとおりです。

© IWATA GODO 2025

ケース 1 は 2024 年 8 月 21 日に公表された、PDPA 違反に基づく初の制裁事例であり、ケース 2 から 6 は、2025 年 8 月 1 日に同時に公表された事案です。

詳細な事実関係や罰金額の算定理由等は公表されておりませんが、同様の事案であっても会社の規模によって罰金額が異なると考えられること、情報処理を委託している場合の委託者の監督義務違反が重く処罰される傾向にあること、DPO の不選任が罰金の加重要素になっている可能性がある等の特徴があるといえます。さらに、電話詐欺業者への漏洩事案が 3 件あります。

ケース 1　商取引オンラインサービスのプロバイダー
- 商取引オンラインサービスのプロバイダーが保有する個人データが電話詐欺業者に漏洩した事案。 - 罰金：700 万バーツ（約 3,220 万円） - 特定された違反行為：適切なセキュリティ対策の欠如／データ侵害の通知の懈怠／DPO 不選任
ケース 2　政府機関とアプリ開発業者
- アプリ開発業者が開発した政府機関のウェブアプリへのサイバー攻撃により、20 万人分の個人データが流出した事案。 - アプリ開発業者及び政府機関への罰金：各 153,120 バーツ（約 70 万円） - 特定された違反行為： ➢ 政府機関による適切なセキュリティ対策の欠如（脆弱なパスワードの使用、リスク評価の実施及びセキュリティ対策の見直しの懈怠、アプリ開発業者との間のデータ処理契約の不存在） ➢ アプリ開発業者による適切なセキュリティ対策の欠如（セキュリティ対策の設計及びデータアクセス制御システム整備の懈怠、リスクアセスメントの不実施、データ漏洩防止措置の不実施）
ケース 3　私立病院及び記録破棄委託業者
- 私立病院が患者の医療記録の破棄を外部委託していたところ、当該委託業者の職員が破棄手順を遵守せず、医療記録を自宅に持ち帰り菓子の包装に使用し、1,000 件以上の医療記録が漏洩した事案。医療記録で包装された菓子の画像がソーシャルメディアに掲載され、PDPC が発見したことから発覚した事案。 - 病院への罰金：121 万バーツ（約 556 万円）、委託業者への罰金：16,940 バーツ（約 78,000 円） - 特定された違反行為：委託業者の個人情報の不正持ち出し及び目的外利用／病院の管理監督義務違反
ケース 4　コンピュータ機器販売大手企業
- コンピュータ機器販売会社が保有する 100 名を超える個人のデータが電話詐欺業者に漏洩した事案。 - 罰金：700 万バーツ（約 3,220 万円） - 特定された違反行為：適切なセキュリティ対策の欠如／データ侵害の通知の懈怠／DPO 不選任

© IWATA GODO 2025

ケース 5　化粧品販売代理店
- 化粧品会社が保有する個人データが電話詐欺業者に漏洩した事案。 - 罰金：250 万バーツ（約 1,162 万円） - 特定された違反行為：適切なセキュリティ対策の欠如／データ侵害の通知の懈怠
ケース 6　玩具会社
- 玩具会社が予約システムの管理をデータ処理業者に委託していたところ、システムへの不正アクセスが行われ、約 20 万件の個人データが不正に変更された事案。 - 玩具会社への罰金：50 万バーツ（約 230 万円）、データ処理業者への罰金：300 万バーツ（約 1,380 万円） - 特定された違反事項：適切なセキュリティ対策の欠如

第4　違反事例を踏まえた特に留意すべき義務の内容

第 3 に挙げた違反事例の多くにおいて違反行為として特定されている、①セキュリティ対策実施義務、②DPO 選任義務、③データ侵害発生の通知義務についてご説明します。

1　セキュリティ対策実施義務

データ管理者は、個人データへの不正なアクセス、利用、改変、収集及び開示を防止するため、適切なセキュリティ対策を実施しなければならないとされています。また、PDPC が定めるセキュリティ対策の最低基準を遵守する必要があります（37 条 1 項）。

データ処理者も、情報管理者の指示に従う義務（40 条 1 項）のほか、データ管理者と同様に適切なセキュリティ対策の実施義務を負います（同条 2 項）。

最低基準については、2022 年 6 月 30 日に公表されたデータ管理者のセキュリティ対策に関する通達[2]に定められています。

[2] 主な内容は次のとおりです。
- セキュリティ対策は適切な組織的対策と技術的対策（必要に応じて物理的対策も含む）で構成され、リスクの大きさ、個人データの収集・利用・開示の性質や目的、データ侵害の影響度を考慮に入れたものとされなければならない。
- セキュリティ対策を構築する際には、重要な情報資産に対する重大かつ潜在的なリスクの特定とその防止、データ侵害脅威の調査・監視及び侵害発生時の対応並びに損害発生時の救済と回復について、リスクレベルに応じて適切に考慮しなければならない。
- セキュリティ対策は、技術的要因、状況、同様の種類のビジネスで受け入れられている基準、データの収集・利用・開示の目的及び実現可能性を考慮して、リスクレベルに応じて個人データの機密性、整合性、および可用性を適切に維持できるものでなければならない。
- 電子形式の個人データに対するセキュリティ対策は、リスクを軽減するために多層的に行われるべきである。具体的には、関連情報システムの様々な構成要素（サーバー、クライアント、ストレージシステム及びネットワークシステムを利用する各種機器、ソフトウェア、アプリケーション等）を、リスクレベルに応じて適切に保護するセキュリティ対策を構築しなければならない。

© IWATA GODO 2025

2　DPO 選任義務

データ管理者及びデータ処理者は、①政府機関の場合、②個人データの取り扱いが大規模であって個人データ又はシステムの定期的な監視を必要とする場合として PDPC が定める場合[3]、及び③中核的業務が思想・宗教・健康情報等のセンシティブ個人データの収集・利用・開示である場合には、データ保護責任者（DPO）を選任しなければならないとされています（41 条）。

3　データ侵害発生の通知義務

データ管理者は、「データ侵害」が発生した場合、データ主体の権利及び自由にリスクをもたらす可能性が低い場合を除き、遅滞なく PDPC に通知しなければなりません（37 条 4 項）。

データ侵害の取り扱いについては、2022 年 12 月 15 日に公表された個人データ侵害の取り扱いの基準と手順に関する通達[4]に詳細が定められています。

- 個人データへのアクセス、使用、変更、修正、削除、開示に関するセキュリティ対策は、適切な本人確認や認証等のアクセス制御、適切なユーザー登録やアクセス権付与等のユーザーアクセス管理、個人データの不正利用等を防止するためのユーザーの責任の定義、個人データのアクセス・変更・収集・消去の履歴を監督可能にする措置の導入を含まなければならない。

[3] 2023 年 9 月 14 日に公表された DPO の選任に関する通達により、以下のとおり具体化されています。

- 個人データの取り扱いが大規模であるため、個人データ処理に定期的な監視が必要かどうかを判断する際には、データ管理者またはデータ処理者の「中核的活動」のみを考慮する。「中核的活動」とは、データ管理者またはデータ処理者の主たる業務に直接関連する不可欠かつ重要な活動を指す。
- 「個人データの定期的な監視を必要とする行為」とは、個人の行動、態度、又は特性（プロファイル）の追跡、監視、分析又は予測に関連する行為を指し、一般的には、定期的かつ体系的な方法で個人データを処理することが含まれる。例としては以下のものが挙げられる：会員カード、公共交通機関カード、電子カード等の利用に関する個人データの収集、契約締結やサービス提供に先立つ信用スコアリング、保険料算定及び詐欺防止等のリスク評価のための個人データ収集、ターゲティング広告を目的とした個人データの収集、安全確保の目的での個人データの収集。
- 個人データの処理が大規模か否かを判断する際には以下の要素を考慮する：処理される個人データの数、及び収集・利用・開示され得る潜在的な個人データ主体の総数に占める、実際に収集・利用・開示された個人データ主体の割合、個人データの種類及び性質、個人データの処理期間、個人データの処理の地位的範囲。10 万人以上のデータ主体の個人データの処理は「個人データの大規模な処理」とみなされる。

[4] データ侵害とは、故意、過失、偶発、無許可、違法行為又はコンピュータ犯罪、サイバー脅威、過失、事故、その他の行為に起因する、個人データの違法又は不正な紛失、アクセス、利用、改変又は開示を引き起こすセキュリティ対策違反を指します。
データ管理者は、個人データ漏洩又はその疑いについて通知を受けた場合、以下の措置を講じる必要があります。

- 情報の信頼性の評価及び関連事実の調査及び当該侵害が個人の権利と自由にリスクをもたらす可能性についての検討（データ侵害評価）
  - ✓ データ侵害評価に当たっては、2022 年 12 月 16 日 PDPC が発行したガイドラインを参考にすることができる。
- PDPC 及びデータ主体への通知（72 時間以内）
  - ✓ データ侵害が発生した場合、データ管理者は、当該侵害が個人の権利と自由に影響を与える可能性が低い場合を除き、侵害を認識してから 72 時間以内に PDPC に遅滞なく通知しなければならない。特定の様式はないものの、通知には、①侵害の性質、関連する個人データ記録の種類と量、②DPO の連絡先、③想定される影響、④是正改善措置を含める必要がある。通知は書面、口頭又は電子メールにより行うことができる。

© IWATA GODO 2025

第5　まとめ

PDPC は漏洩事案に対して積極的に行政罰を科し、それを公表することにより、PDPA 遵守のより厳格な遵守を求めるように舵を切っています。これまでの罰金額は、1 件 3000 万円を超えるものもあり、第 4 で挙げた 3 つの重要な義務を中心に、社内の個人情報保護体制及びシステムについて、今一度見直しを行うことをお勧めいたします。

- ✓ データ侵害が個人の権利と自由に影響を与えるリスクが高い場合、データ管理者は個人データ侵害を認識した後、遅滞なくデータ主体に通知しなければならない。通知には、①～④に加え、損害に対する救済措置を含める必要がある。個別通知が原則であるが、個別通知が不可能な場合には、SNS や公共メディア等により集団又は一般に対する通知・公表を行うこともできる。
- ✓ データ処理者も、個人データの漏洩を認識した後、遅滞なく、72 時間以内にデータ管理者に通知しなければならず、データ管理者はその旨の条項をデータ処理契約に含める必要がある。

© IWATA GODO 2025

【執筆者】

松田 章良
Email: amatsuda@iwatagodo.com

2006 年東京大学法学部卒業、2015 年 Columbia Law School（LL.M.）修了（Harlan Fiske Stone Scholar 受賞）。2008 年弁護士登録、2019 年 NY 州弁護士登録。個人情報保護、国際関係法務・渉外業務（取引）、IT・サイバー法に係る案件、国際仲裁・国際紛争解決案件、大規模かつ複雑な訴訟・紛争解決案件を主に取り扱う。

別府 文弥（弁護士）
Email: fbeppu@iwatagodo.com

2010 年東京大学法科大学院修了、2017 年 University of California, Berkeley School of Law (LL.M.)修了。
2011 年弁護士登録、2018 年カリフォルニア州弁護士登録。
Drew & Napier LLC, シンガポールオフィス駐在。
米国・東南アジアを始めとするクロスボーダー及び日本国内の M&A 取引、紛争解決、その他企業法務全般（国内・国際商取引、業規制、労働法関係）に関する法的助言を行う。

深津春乃（弁護士）
E-mail: haruno.fukatsu@iwatagodo.com

2016 年京都大学大学院法学研究科修了。2025 年 University of Michigan Law School (LL.M.)修了。2017 年弁護士登録。2025 年 9 月～タイ Tilleke&Gibbins.法律事務所駐在。クロスボーダー及び日本国内のコーポレート案件、M&A 取引を主として担当するほか、紛争解決、業規制を含む企業法務全般に関し広く法的助言を行う。

岩田合同法律事務所

1902 年（明治 35 年）、司法大臣や日本弁護士連合会会長を歴任した故・岩田宙造弁護士が「岩田宙造法律事務所」を創立したことに始まる、我が国において最も歴史のある法律事務所の一つです。創立当初より、我が国を代表する企業等の法律顧問として広範な分野で多数の企業法務案件に関与しております。弁護士 110 余名のほか、日本語対応可能な外国法事務弁護士（中国法、フランス法、米国法）も所属し、特別招聘顧問として元最高裁長官大谷直人氏が在籍しております。

〒100-6315 千代田区丸の内二丁目 4 番 1 号　丸の内ビルディング 15 階
岩田合同法律事務所　広報： newsmail@iwatagodo.com

※本ニュースレターは一般的な情報提供を目的としたものであり、法的アドバイスではありません。また、その性質上、法令の条文や出展を意図的に省略している場合があり、また情報としての網羅性を保証するものではありません。個別具体的な案件については、必ず弁護士にご相談ください。

© IWATA GODO 2025