WEBINAR ／ YouTube 解説

タイの個人情報保護法（PDPA）
最新実務アップデート

2024 ～ 2026 年の執行強化・越境移転・本人請求・ AI ・法改正
― タイに拠点を持つ日系企業のための実務ポイント

Privacy in Action ― 書類から「動く仕組み」へ

弁護士法人三宅法律事務所
弁護士　渡邉雅之
2026 年 9 月

本日の構成

今日の流れ： 6 つのパート

序

全体像・日本法／ GDPR との比較

なぜ日系企業に関係するのか／日本の感覚で間違えやすい点

1

執行の本格化

2024 ・ 2025 年の制裁／ 72 時間対応／ World 事件

2

法的根拠・マーケ・ DPO

「とりあえず同意」からの転換／ ROPA ／独立性

3

越境移転・ DSAR ・認証

SCC ・ BCR ／ 9 月 14 日施行の DSAR 告示／認証制度

4

AI ・法改正

AI ガイドライン案／第 24 条の再構成

★

まとめ・アクション

優先点検 7 項目／ 30 日・ 90 日でやること

本日の構成

先に押さえる略語ガイド

PDPA
Personal Data Protection Act

タイ個人情報保護法

PDPC
Personal Data Protection Committee

タイ個人情報保護委員会（監督当局）

GDPR
General Data Protection Regulation

EU 一般データ保護規則

DPO
Data Protection Officer

データ保護責任者

DPA
Data Processing Agreement

データ処理契約（委託先との契約）

ROPA
Record of Processing Activities

処理活動記録（データ処理の台帳）

LIA
Legitimate Interest Assessment

正当な利益の評価

DPIA
Data Protection Impact Assessment

データ保護影響評価

DSAR
Data Subject Access Request

本人からのアクセス請求

SCC
Standard Contractual Clauses

標準契約条項（越境移転）

BCR
Binding Corporate Rules

拘束的企業準則（グループ内移転）

ASEAN MCC
ASEAN Model Contractual Clauses

ASEAN モデル契約条項

序章

「書類はある」だけでは、もう足りない

72 時間

侵害を PDPC へ通知

第 37 条 (4)

30 日

アクセス請求への回答

第 30 条・DSAR 告示

2,150 万バーツ

行政制裁金の累計（2024 ～ 25 年）

PDPC 公表

2,672 件

PDPA への苦情（2026 年 1 月時点）

PDPC 事務局

PDPA 対応の焦点は、文書から「動く仕組み」へ

序章

なぜ日系企業に関係するのか：データは「チェーン」になる

本社がタイ子会社の従業員情報を管理

顧客データをグループ横断でマーケ利用

予約・ EC ・会員管理を外部システム会社へ委託

生成 AI ・分析ツールに現地データを投入

→ タイの法律でも、日本本社・委託先・クラウド契約・ AI 利用ルールまで影響する（域外適用：第 5 条）

序章

まず押さえる 4 つの役割:「誰が管理者で、誰が処理者か」

本人

Data Subject

顧客・従業員など
データで識別される個人

第 6 条

管理者

Data Controller

処理の目的・手段を
決定する者

第 37 条・第 39 条ほか

処理者

Data Processor

管理者の指示で
代わりに処理する者

第 40 条（直接の義務）

DPO

Data Protection Officer

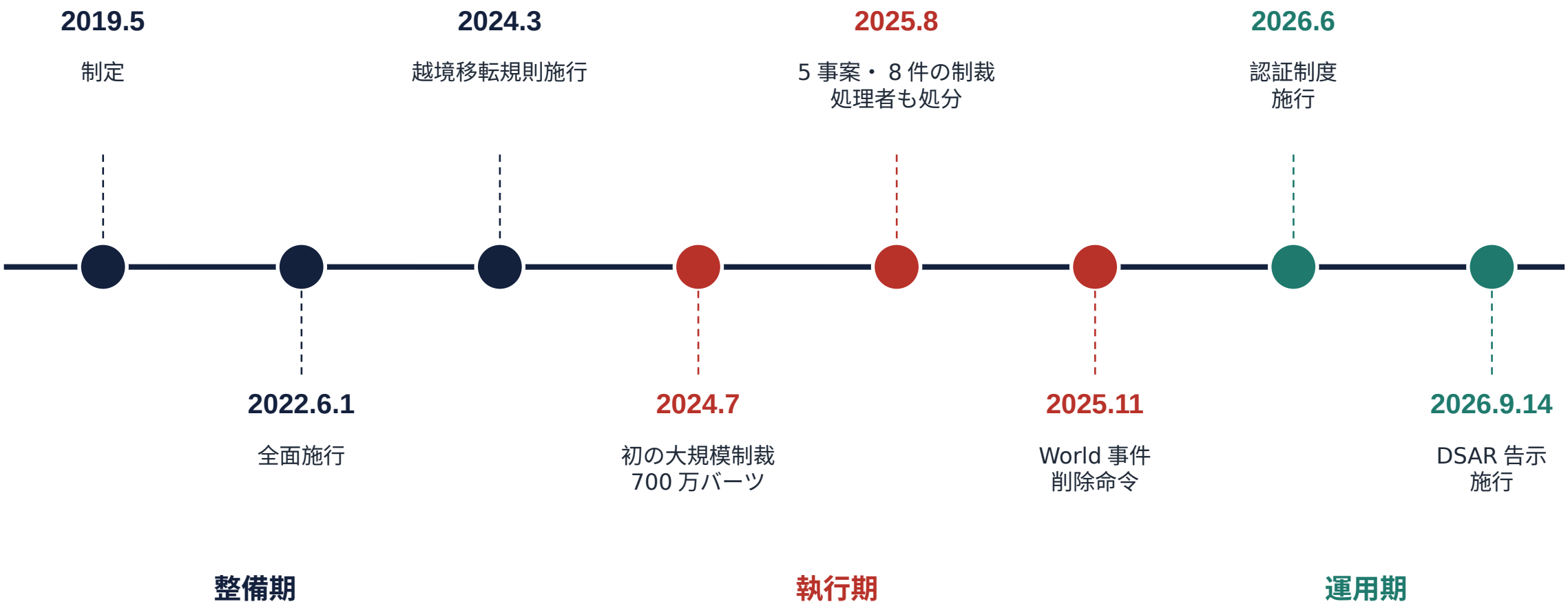
遵守の監督・助言・
当局との窓口

第 41 条・第 42 条

ポイント: システム会社・クラウドは「外注先」ではなく、処理者として直接義務を負う主体。役割整理が DPA （データ処理契約）・漏えい報告・越境移転の出発点。

序章

2019→2026 年：タイ PDPA の歩み



序章

2026 年の 3 つの潮流：ニュースはこの地図で整理する

第 1 章

① 執行の本格化

- 制裁金・是正命令
- 処理者への直接処分
- 漏えい報告遅延への厳格評価

第 2 ・ 3 章

② 下位規則・実務化

- 法的根拠・マーケ・ ROPA 案
- DPO ・越境移転・ BCR
- DSAR 告示・認証制度

第 4 章

③ 法改正・新領域

- 第 24 条の再構成（改正案）
- AI ガイドライン案
- 生体情報・同意の実質審査

注意：「拘束力ある告示」「ガイドライン案」「改正案」を混同しない

日本・ GDPR ・タイ： ３つの法律を「ひと言」で

日本（個人情報保護法）

「目的＋同意」型

- 目的を特定・通知
- 目的外利用と第三者提供は原則同意
- 要配慮個人情報は取得にも同意
- 「正当な利益」の根拠はない

第 17 ・ 18 ・ 20 ・ 21 ・ 27 条

EU （ GDPR ）

「根拠」型

- すべての処理に法的根拠が必要
- 同意は 6 つの根拠の一つにすぎない
- 特別な種類は原則禁止＋例外

第 6 条・第 9 条

タイ（ PDPA ）

「同意＋例外」型

- GDPR がモデル
- 条文上は同意が出発点
- 同意不要の場合を例外として列挙
- センシティブは明示的同意

第 19 ・ 24 ・ 26 条

たとえると　日本：要配慮の取得・目的外利用・第三者提供は同意　／　**GDPR ・タイ：処理ごとに“許可証”が要る**

比較表：タイ PDPA は「GDPR にかなり近い」

項目	日本（個人情報保護法）	EU （GDPR）	タイ（PDPA）
監督当局	個人情報保護委員会（独立の行政委員会）	各国の監督機関（SA）＋ EDPB	PDPC ＋事務局／専門委員会が制裁
処理の基本	目的特定・通知＋目的外利用と提供は同意	6 つの法的根拠が必要（第 6 条）	同意原則＋例外列挙（第 19 ・ 24 条）
「正当な利益」	なし（令和 8 年改正でも不導入）	あり（第 6 条 1 項 (f)）	あり（第 24 条 (5)）
センシティブ情報	要配慮：取得に本人同意（第 20 条 2 項）	原則禁止＋例外（第 9 条）	原則明示的同意（第 26 条）
漏えい報告	速報 3 〜 5 日・確報 30 日（第 26 条）	72 時間（第 33 条）	**72 時間（第 37 条 (4)）**
本人請求の回答	遅滞なく（第 33 条）	1 か月＋ 2 か月延長（第 12 条 3 項）	30 日＋ 30 日延長（第 30 条・告示）
DPO	法定義務なし	一定の場合に義務（第 37 条）	**一定の場合に義務（第 41 条）**
委託先	委託元に監督義務（第 25 条）	処理者に直接義務（第 28 条）	**処理者に直接義務（第 40 条）**
越境移転	同意・体制整備・十分性国（第 28 条）	十分性・ SCC ・ BCR （第 44 〜 49 条）	リスト未公表→ BCR ・ SCC （第 28 ・ 29 条）
制裁	課徴金を新設（令和 8 年改正・施行前）／刑事罰	最大 2,000 万ユーロ／全世界売上高 4%	最大 500 万バーツ＋懲罰的賠償
域外適用	あり（第 171 条）	あり（第 3 条 2 項）	あり（第 5 条）

GDPR と同じ・ほぼ同じ　　タイ独自の特徴

→ タイ PDPA は日本法より「GDPR にずっと近い」

序章　比較

日本の感覚で間違えやすい 6 つのポイント

1

日本の感覚

✕ 利用目的を公表していれば OK

タイでは　**処理ごとに法的根拠が必要（第 24 条）**

2

日本の感覚

✕ 漏えいの速報は 3 〜 5 日以内

タイでは　**72 時間以内に PDPC へ通知（第 37 条 (4)）**

3

日本の感覚

✕ 開示請求は「遅滞なく」

タイでは　**30 日以内＋手続告示（2026 年 9 月 14 日施行）**

4

日本の感覚

× DPO は任意

タイでは　**一定の場合は選任義務（第 41 条）**

5

日本の感覚

✕ 日本は十分性認定国だから移転 OK

タイでは　**それは EU との関係。タイではリスト未公表**

6

日本の感覚

✕ 課徴金はこれから（日本は施行前）

タイでは　**行政制裁金をすでに現に賦課・処理者も**

01

執行の本格化

2024 年・ 2025 年の制裁事例から、当局が何を見ているかを読み解く

2024 年：最初の大規模制裁が示したこと

オンライン販売事業者

700 万バーツ

顧客 10 万人超／漏えいデータが詐欺電話に利用された可能性

決定：2024 年 7 月 31 日（専門委員会）
公表：2024 年 8 月 21 日（MDES）

安全管理措置の不備

第 37 条 (1)

アクセス制御・リスク評価が不十分

DPO 未選任

第 41 条 (2)

大規模処理なのに選任なし

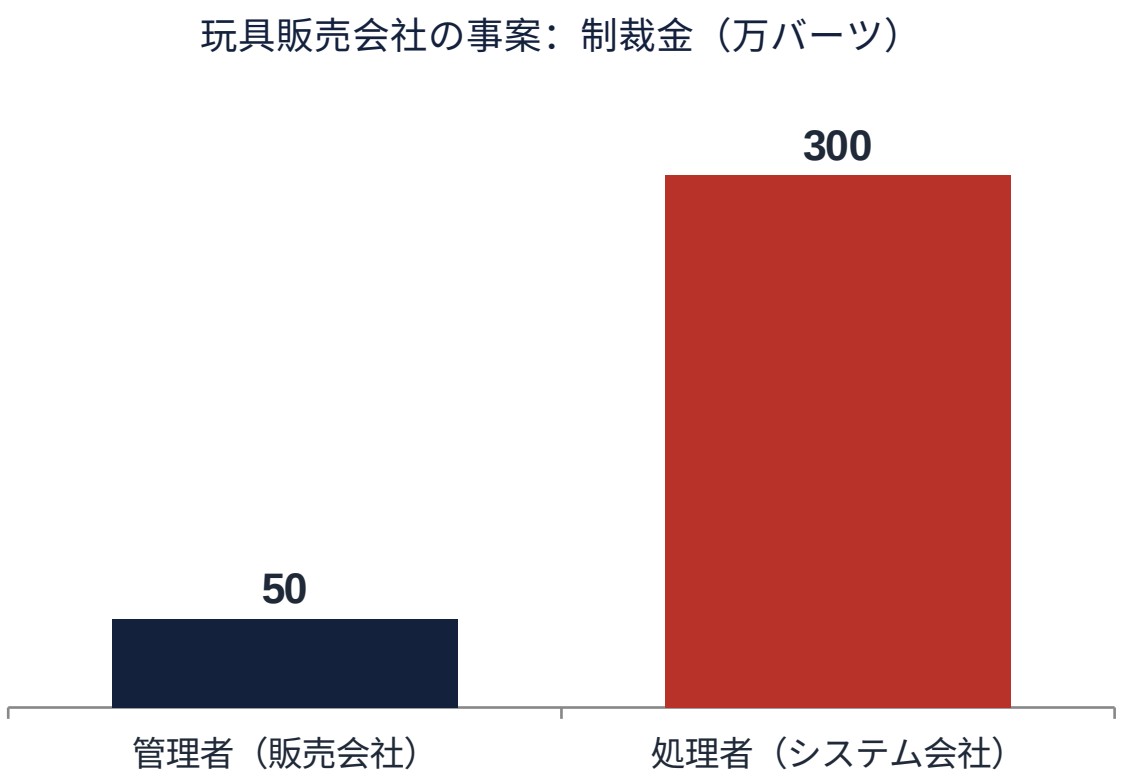
侵害通知の懈怠

第 37 条 (4)

法定期間内に PDPC へ通知せず

→ 問われたのは「防ぐ・任せる・報告する」仕組みの不在

2025 年：管理者だけでなく処理者も処分対象に



処理者は管理者の 6 倍

5 事案 8 件 約 1,450 万バーツ

2025 年 8 月 1 日公表／累計 約 2,150 万バーツ

- 政府機関 Web アプリ： 20 万人超流出 → 機関と開発会社の双方に各 153,120 バーツ
- DPA 未締結・委託先監督の不足・安全管理不足を具体的に認定
- 是正命令＋ 30 日以内の履行。不履行なら 50 万バーツ以下の制裁金（第 89 条）

委託先任せでは足りない。処理者管理そのものが執行対象。

繰り返された 4 つの違反類型：そのまま内部監査の項目に

安全管理措置

第 37 条 (1)

アクセス制御・パスワード・リスク評価

Q. 管理者権限は誰が持ち、いつ見直した?

72 時間報告

第 37 条 (4)

侵害認識後の評価・判断・通知の遅れ

Q. 夜間・週末に検知したら誰が判断する?

DPO

第 41 条

選任義務があるのに未選任・名目だけ

Q. 選任要否の判断は記録されている?

DPA ・委託先監督

第 40 条

委託契約の欠如・監督記録の不足

Q. 主要委託先の DPA 一覧をすぐ出せる?

個人データ侵害：　72 時間の勝負

0h

検知

ログ・通報・委託先からの連絡

～ 24h

初期評価

対象データ・件数・影響範囲

～ 48h

報告要否判断

権利・自由へのリスク評価

～ 72h

PDPC 通知

高リスクなら本人にも通知

盲点は委託先：処理者の報告が遅れると、管理者の 72 時間が消える

DPA に明記すべき事項：報告期限（例：認識から 24 時間以内）／報告内容／調査協力義務／ログ等の証跡提出

PDPA 第 37 条 (4)（管理者の PDPC ・本人通知）／第 40 条 (2)（処理者の管理者への通知）

制裁体系：行政制裁金だけではない

行政制裁金

管理者 第 82 ～ 84 条
処理者 第 85 ～ 87 条

上限 100 万／300 万／500 万バーツ
複数違反なら合計は上限超も

民事責任

第 77 条・第 78 条

事業者側が免責事由を立証
実損＋ 2 倍以内の懲罰的損害賠償

刑事罰

第 79 条以下

センシティブデータの違法な利用等
最大 1 年・100 万バーツ（第 79 条）
職務上の漏示（第 80 条）・役員（第 81 条）

＋ 命令不履行に 50 万バーツ以下の制裁金（第 89 条）＋ 本人対応 ＋ レピュテーション

World （旧 Worldcoin ）事件：生体情報と「自由な同意」

虹彩情報

センシティブデータ（第 26 条）
明示的同意が原則

→

WLD の付与

経済的インセンティブと
引き換えにスキャン

→

同意の実質審査

理解・任意性・説明の十分性を
総合的に評価

2025.11.24　PDPC が収集停止・削除／破棄を命令

2026.1　DSI 等が 120 万人超の虹彩情報取得を公表

教訓：同意は「チェック」ではなく、理解・自由意思・説明可能性

02

法的根拠・マーケティング・ DPO

「とりあえず同意」から、処理ごとに根拠を選び、記録する時代へ

法的根拠：「とりあえず同意」からの転換

これまで

全部、同意を取ればよい

撤回されたら止まる／雇用関係では任意性が疑われる

→

これから

処理ごとに根拠を選ぶ

選択の過程を記録し、 Privacy Notice で説明する

第 24 条が定める根拠（同意以外）と具体例

(1) 研究・統計
統計目的の分析

(2) 生命・身体
緊急時の医療情報

(3) 契約履行
給与計算・配送

(4) 公共の利益
公的任務の遂行

(5) 正当な利益
防犯カメラ・不正防止

(6) 法的義務
税務・社会保険

法的根拠を選ぶ 5 ステップ（2026 年 7 月ガイドライン案）

例 A：既存顧客に類似サービスを案内

- 候補：正当な利益（第 24 条 (5)）
- 確認：合理的な予測可能性・拒否手段・影響の小ささ
- 記録： LIA （正当な利益の評価）を作成し保存

例 B：別商品・グループ会社の広告に利用

- 候補：同意、又は別根拠の精査
- 確認：予測可能性を超えるか・第三者提供・越境移転
- 記録：取得経路・提供権限も確認

ROPA は「台帳」からアカウンタビリティの背骨へ

マーケティング利用：本人の「予測可能性」が分かれ目

低リスク寄り

既存顧客に類似の商品・サービスを案内

注意が必要

別商品・新サービスの案内

高リスク寄り

グループ会社・ブローカーから取得／プロファイリング・ AI

本人の予測可能性から遠ざかる →

- **本体サービスとマーケ同意を分離**
- **事前チェック・包括同意を避ける**
- **拒否しても本体サービスを止めない**
- **第三者取得は提供権限を確認**

DPO： 選任義務よりも「独立性」が問われる

第 41 条

選任義務

政府機関／大規模な定期的監視／
センシティブデータが中核的活動

第 42 条

独立性・利益相反

兼務は利益相反なき範囲で／
職務を理由とする解任禁止／
最高経営責任者へ直接報告

実務

機能しているか

報告ルート・リソース・
兼務職務の整理を記録

利益相反が生じやすい兼務

- CEO
- CFO
- 人事責任者
- マーケ責任者
- IT 設計責任者

DPO は「担当者」ではなく、個人データ処理を独立して監督する「機能」

03

越境移転・ DSAR ・認証

日本本社への移転、 9 月 14 日施行のアクセス請求手続、新しい認証制度

越境移転：日本本社への移転も「当然 OK」ではない

十分性認定国リスト

2026 年 9 月時点で未公表

→「日本だから当然 OK」とは言えない

第 28 条

十分性のある国へ

原則ルート。ただしリスト未公表

第 28 条ただし書

個別の例外

法令・同意・契約履行など
個別・限定的な移転向け

第 29 条

BCR

グループ内の拘束的企業準則
PDPC の審査・認証

第 29 条

SCC 等の保護措置

契約による適切な保護措置
本社移転・クラウドの実務標準

SCC と BCR：どちらを使うか

SCC

Standard Contractual Clauses

- 二社間・限定的な移転
- タイ子会社 → 日本本社
- クラウド・委託契約で早く整備
- ASEAN MCC ・ EU SCC をベースにする例

BCR

Binding Corporate Rules

- 多国籍グループ全体の移転
- 反復的・大規模な内部移転
- BCR-C ／ BCR-P 、タイ語文書、審査最長 180 日
- 既存の EU/UK BCR を転用できる可能性

実務感：通常の日系企業は「SCC ＋ DPA ＋越境移転台帳」から整備するのが現実的

DSAR： 2026 年 9 月 14 日から手続が具体化

施行日

2026.9.14

PDPA 第 30 条のアクセス請求手続に関する告示（B.E. 2569）
制定 7 月 6 日／官報掲載 7 月 16 日／掲載 60 日後に施行

対象①　アクセス・写しの請求
対象②　同意なく取得したデータの取得元の開示

受付手段	直接提出＋書留郵便を最低限。電子手段の追加は可
本人確認	本人・法定代理人・委任を受けた代理人等を確認
回答期限	原則 30 日以内。理由を通知して最大 30 日延長
拒否・手数料	拒否事由・部分開示・手数料の規律
記録保存	請求内容と対応結果を 2 年以上保存

DSAR 対応フロー： 30 日でここまで行う

← 原則 30 日（理由通知で最大 30 日延長） →

拒否できる場合（第 30 条第 2 項）

法令・裁判所の命令により認められ、**かつ**
他人の権利・自由に悪影響を及ぼす場合

拒否理由は ROPA に記録（第 30 条第 4 項・第 39 条）

事前に決めておくこと

- 検索対象のシステム
- 一次対応部署と最終判断者
- タイ語請求への対応者

PDPA 認証制度：「書類」から「成熟度」を示す仕組みへ

評価基準

128 項目

10 領域／告示 2 本（評価基準＋申請手続）
2026 年 6 月 18 日 官報掲載・即日施行

任意の制度／認証＝免責ではない

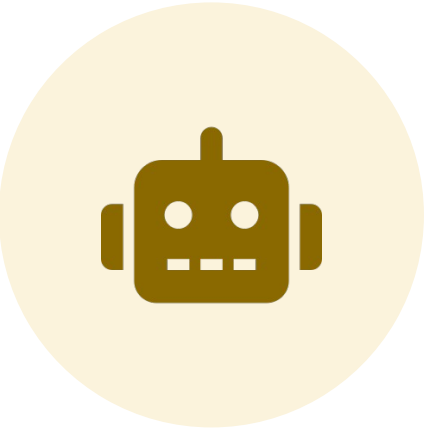
01 ガバナンス	02 方針・手続
03 人材・研修	04 本人の権利
05 透明性	06 ROPA ・根拠
07 DPA ・共有	08 DPIA ・リスク
09 セキュリティ	10 侵害対応

→ 今日の論点がそのまま審査項目に

04

AI・法改正

AI ガイドライン案と、第 24 条を再構成する PDPA 改正法案



AI と個人データ：新ルールを待たずに PDPA は適用される

確認すべきこと

- DPA
- 越境移転
- 安全管理措置
- DPIA の要否
- 社内 AI 利用ルール

2026.2.17	PDPC： AI ガイドライン案公表
2026.3.13–19	第 2 次案の意見募集
現時点	未確定・拘束力なし／ ETDA は AI 法制を別途検討

「AI ルール待ち」は誤り。個人データを入れる以上、既存の PDPA が今すでに適用される。

PDPA 改正案：第 24 条が GDPR 型に近づく可能性

現行法

同意が原則
＋
同意なしで処理できる例外を列挙

→

改正案

- 同意
- 契約履行
- 法的義務
- 公共の利益
- 正当な利益

＝ 並列の根拠（GDPR 第 6 条型）

意見募集：2026 年 7 月 16 日～8 月 15 日（2017 年憲法第 77 条）／成立すれば官報公布の翌日施行

現行法・告示	ガイドライン案	改正案
拘束力あり	拘束力なし・事実上の基準	未成立

まとめ

日系企業の優先点検事項 7 つ

1. 72 時間以内の侵害評価・報告体制
2. 処理者との DPA と委託先監督
3. タイ国外移転の根拠・ SCC ・ BCR
4. DPO の選任要否・独立性・利益相反
5. マーケティングの法的根拠と LIA
6. DSAR の受付・ 30 日対応・ 2 年保存
7. 生体情報・ AI の同意・透明性・ DPIA

最優先は ①漏えい ②委託先 ③越境移転

まとめ

まず何をするか： 30 日・ 90 日アクション

30 日以内　確認する

- 漏えい時の連絡網（夜間・休日含む）
- 主要委託先の DPA の有無
- 日本本社へのデータ移転の棚卸し
- DSAR 窓口と責任部署の決定

90 日以内　整備する

- DPA ／ SCC を更新（報告期限を明記）
- ROPA を実態に合わせて更新
- LIA ・ DPIA のテンプレート作成
- DPO の独立性と報告ルートの確認

ポイント：完璧な文書より、まず「動く最低限」を作る

結論

タイ PDPA は「Privacy in Action」へ

説明できる

根拠を本人と当局に

記録できる

ROPA ・ LIA ・ DPA ・台帳

動ける

漏えい・請求・委託先事故

2026 年以降の焦点は、アカウンタビリティと実効性。

チャンネル登録をお願いします

あたらしい法律情報

法務・コンプライアンス向けウェビナー動画を毎日１～２本配信中

youtube.com/channel/UCFrR7Ch7FnVFvw9ckbjR5ag

ご相談・お問い合わせ

弁護士法人三宅法律事務所　弁護士　渡邉雅之

03-5288-1021

m-watanabe@miyake.gr.jp

出典

主な参照資料

- Personal Data Protection Act B.E. 2562 (2019)（英訳： MDES ）
- MDES 公表（ 2024 年 8 月 21 日）： オンライン販売事業者への 700 万バーツ制裁
- タイ政府・ PDPC 公表（ 2025 年 8 月 1 日）： 5 事案・ 8 件の行政制裁
- Royal Gazette： DSAR 告示 B.E. 2569 （ 2026 年 7 月 16 日掲載・ 9 月 14 日施行）
- Royal Gazette： PDPA 認証制度告示 2 本（ 2026 年 6 月 18 日掲載）
- Royal Gazette： BCR 審査・認証規則 B.E. 2568 （ 2026 年 2 月 17 日掲載）
- DSI ・ SEC： World （旧 Worldcoin ）虹彩情報に関する公表資料
- タイ国会：憲法第 77 条に基づく意見募集（ PDPA 改正法案、 2026 年 7 月 16 日〜 8 月 15 日）
- PDPC 事務局：法的根拠・マーケティング・ ROPA 等ガイドライン案（ 2026 年 7 月 7 日）、 AI ガイドライン案（ 2026 年 2 月 17 日）
- 日本：令和 8 年改正個人情報保護法（令和 8 年法律第 56 号）／ EU： GDPR
- Tilleke & Gibbins 、 Baker McKenzie 、 Herbert Smith Freehills Kramer 、 Chambers 等の実務解説

本資料は 2026 年 9 月時点の公開情報に基づく一般的な解説であり、個別案件に関する法的助言ではありません。