マレーシア：新たな個人データ保護ガイドライン

概要

2025年の意見公募手続を経て、マレーシアの個人情報保護委員会（Personal Data Protection Commissioner, PDPC）は以下の新たなガイドラインを公表しました：

- データ保護影響評価（Data Protection Impact Assessment, DPIA）
- 設計によるデータ保護（Data Protection by Design, DPbD）
- 自動化された意思決定およびプロファイリング（Automated Decision-Making and Profiling, ADMP）

本クライアントアラートでは、これら3つのガイドラインの概要を示すとともに、マレーシアの「2010年個人情報保護法（Personal Data Protection Act, PDPA）」の適用を受ける組織にとっての重要なポイントを解説します。

目次

上記の見出しをクリックすると、そのセクションに直接移動します。

DPIAガイドライン

DPIAの概念は、PDPC通達第1/2025号に基づくデータ保護責任者（Data Protection Officer, DPO）の責務の一つ、すなわち、PDPCが随時定める要件に従ってDPIAの実施に関する支援および助言を提供し、その遵守状況を監視することに由来しています。

DPIAガイドラインに定められているこれらの要件は、以下のとおり整理されています。

❖ DPIAとは何か？

DPIAとは、本質的に、計画されている処理業務における個人データ保護上のリスクを分析し、軽減するためのプロセスです。これには、組織の機能、要件およびプロセスに基づき、当該リスクを特定、評価および管理することが含まれます。

❖ 誰がDPIAを実施する責任を負うか？

データ管理者、特にその経営陣が最終的な責任を負います。各データ保護責任者（DPO）は、カスタマイズされたDPIAテンプレートまたはチェックリストを作成し、DPIAの実施要否を判断し、DPIAの実施およびリスク軽減措置について助言を行います。

❖ どのような場合にDPIAが必要か？

処理業務がデータ主体の個人データの保護に対して高いリスクをもたらすおそれがある場合に実施が必要となります。具体的には以下のとおりです。

- 定量的基準に基づき高リスクとみなされる場合：10,000人を超えるデータ主体に係る機微な個人データ[1]（財務情報データを含む）の処理、または20,000人を超えるデータ主体に係るその他の個人データの処理を行う場合。

[1] PDPAにおいて「機微な個人データ」とは、本質的に、(a) 身体的もしくは精神的な健康状態、(b) 政治的見解、(c) 宗教的またはそれに類する信条、(d) 犯罪の実行もしくはその嫌疑、または (e) 生体データに関する個人データを指します。

- データ保護責任者（DPO）が定性的基準に基づき最善の判断を行う場合：データ主体に対する潜在的な法的影響もしくは重大な影響を及ぼす可能性がある場合、データ主体の体系的な監視のを伴う場合、革新的な技術の利用がある場合、児童や脆弱な個人を対象とする場合等。

DPIAの目的は、組織が個人データの処理を開始する前の段階で、データ保護をリスク評価における重要な焦点として位置付けることにあります。

❖ DPIAはどのように実施すればよいか？

DPIAは、以下の5つのステップで構成されます（DPIAガイドラインに参考テンプレートが掲載されています）。

- 処理業務（性質、範囲、状況、目的）を記述する。
- 処理業務の適法性、必要性および相当性を評価する。
- データ主体の個人データの保護に対する具体的なリスクを特定し、分析する。
- 特定された具体的なリスクに対処するための措置を検討する。
- 当該処理業務の全体的な残存リスクレベルを評価する。

❖ DPIAの実施後はどうすべきか？

- 処理業務の継続の有無およびその方法について、経営陣に報告し、意見を求める。
- 特定されたリスク軽減措置を実施する。
- 2年間の有効期間が満了した時点で、DPIAを改めて実施する。
- 処理業務の終了から少なくとも2年間、関連する記録を保管し、PDPCの要請があった場合には、当該記録を検査のために提示する。

DPbD ガイドライン

DPbDは、PDPAに基づく既存の7つの個人データ保護原則の実施を中核としています。これには、データ処理活動の**ライフサイクル全体**に**適切な技術的および組織的措置を組み込むことが**含まれます。

各個人データ保護原則について、DPbDガイドラインは、拘束性のない非網羅的な概念、適用例およびチェックリストを提示しており、組織は自社の個人データ処理業務や具体的なリスク特性に応じてこれらを適用・調整することができます。これらは主に、以下のDPbD要素に基づいています。

プロアクティブ性	エンドツーエンドの保護	透明性	ユーザー中心主義
•リスクを事前に予測・防止するため、ガバナンスとリソースを確立し、データの利用を最小限に抑えて、デフォルトで個人データを保護するシステムを設計する。	•取得、利用、保存および廃棄を含む、対象となる個人データのライフサイクル全体が、個人データ保護原則に準拠していることを確保する。	•個人データの取扱いについて誠実に説明し、かつ実務との整合性を示すことができる体制を整備することで、説明責任を示す。	•個人データが最終的にデータ主体に帰属することを認識し、データ主体の利益やニーズを踏まえて、製品、サービス、システムおよびプロセスを意識的に設計する。

さらに、DPbDガイドラインは、DPbDが**個人データ管理に関する原則重視かつ予防的なアプローチを採用する企業文化の**確立を意味するとしており、当該考え方は組織全体に適用され、製品、サービス、ガバナンスおよび業務に反映されるべきであるとしています。この目的のために、以下が含まれます。

- 経営陣が高い基準を設定し、これを徹底する明確なコミットメントを示す。
- すべてのステークホルダーが、データ保護基準の継続的な改善に取り組む文化を醸成する。
- 現在の設計および実務における課題を特定し、問題発生前に体系的かつ予防的に対応するプロセスを整備する。

ADMPガイドライン

ADMPには、別個でありながら関連する2つの概念が含まれます：

自動意思決定（ADM）

人の関与なし（関与が極めて限定的な場合、例えば、単に処理対象のデータ入力のみ行う場合を含みます）に、完全または部分的に自動化された手段を用いて意思決定を行うプロセスを指します。

プロファイリング

個人データの自動的な処理により、特定のデータ主体に関する側面を評価し、とりわけ当該主体に関する側面を分析または予測する行為を指します。

ADM またはプロファイリングを実施する前に、前述の DPIA ガイドラインに従って、**まず DPIA を実施する必要があります**。

さらに、ADMP がデータ主体に法的効果（例：契約の解除）をもたらす場合、またはデータ主体に重大な影響（例：長期的な影響）を及ぼす場合、データ管理者は以下の**要件を**遵守する必要があります。

- ADMPの処理を行うために、PDPA（例：明示的な同意に関する第40条、または機微な個人データの処理に関するその他の例外）への準拠を確保する。
- PDPA第7条に基づき、ADMPの処理についてデータ主体に書面による通知を行う。当該通知は容易にアクセス可能であり、ADMPの進展に応じて迅速に更新する。
- データ主体がPDPA第38条に基づく同意の撤回権を行使できるよう、アクセス可能で簡便かつ利用しやすい仕組み及び手続きを整備する。
- データ主体に対し、同意を撤回する権利について、当該権利を行使するために利用可能な仕組みおよびプロセスを通知する。

重要なポイント

これらの動向は、マレーシアにおける個人データ保護の枠組みが成熟しつつあることを反映しており、個人データの保護がいかにして組織にとって重要な市場差別化要因となり得るかを示しています。したがって、未対応の場合には、以下の対応を実施する必要があります。

❖ 高リスクの個人データの処理を中心に、データ処理およびガバナンスの枠組みの中に**DPIAの実施要件を**速やかに**組み込むよう**努める。
❖ ADM（自動意思決定）およびプロファイリングを実施している、または今後導入予定の組織は、**遵守すべき追加要件に留意し、**個人データ保護に関する通知だけでなく、ワークフローや顧客／ユーザーの体験の見直しを行う。
❖ データ処理およびガバナンスのいずれの段階においても、**マルチステークホルダーチーム**（例：製品設計、事業、データセキュリティ、IT チーム）**と協力し**、組織が保有する既存のデータセットを活用する製品・サービスの開発等において**DPbD の原則を組み込む**。

*****

本法務アップデートは、シニア・アソシエイトのChun Hau Ngが寄稿しました。

お問い合わせ

Serene Kan
パートナー
serene.kan@wongpartners.com