マレーシア個人情報保護法改正に伴う DPO 選任義務・データ漏えい通知義務
～最新ガイドラインに基づく解説～

2025 年 4 月
One Asia Lawyers Group Malaysia Team
日本法弁護士　橋本 有輝
Heng Zhenhung

1.　はじめに

2025 年 2 月 25 日、マレーシアの個人情報保護委員（Personal Data Protection Commissioner）は、マレーシア個人情報保護法（Personal Data Protection Act 2010、以下「PDPA」）に基づき、個人情報を取り扱う組織に対して新たなコンプライアンス義務を導入する 2 つの主要なガイドラインを発出した。これらは、「データ保護責任者（Data Protection Officer）の任命に関するガイドライン」および「データ漏えい通知に関するガイドライン」であり、いずれも該当する PDPA 改正法と共に 2025 年 6 月 1 日より施行される予定である。

マレーシアで事業を展開する外国企業、または子会社、支店、サービスプロバイダー、越境移転を通じてマレーシアの個人情報を取り扱う企業は、これらの変更に速やかに対応する必要がある。マレーシアにおいても重大な情報漏洩事故が発生した経緯もあり、これら改正法及びガイドラインを不遵守の場合、刑事罰や企業の信用失墜といった重大な影響が生じる可能性があることに留意されたい。

2.　データ保護責任者（DPO）の任命

(1)　DPO 選任義務を負う企業

まず初めに、DPO の選任義務は、マレーシアにおける全ての企業に課される義務ではないことに留意が必要である。

この義務を負うのは、その企業が行う個人情報の取扱活動が以下のいずれかの条件を満たす場合である。

- 取扱対象となる個人情報の主体が 2 万人を超える場合
- 財務情報や健康情報を含む機微な個人情報を、1 万人を超える者について取扱う場合
- 個人に対する定期的かつ体系的な監視を伴う取扱いが行われている場合

なお、上記最後の部分にある「定期的かつ体系的な監視」には、行動ターゲティング広告、モバイルアプリケーションやウェアラブル端末を通じた健康データの追跡、または住宅・商業環境における自動化システムの利用などが含まれる。これに対し、ポイントカードや会員プログラムの管理については、購入行動の監視を目的とせず、純粋にデータ主体のアカウント管理のために行っている場合には、「定期的かつ体系的な監視」を要する活動とはみなされない可能性がある。

(2) DPO の資格要件

ガイドラインを要約すると DPO の資格要件は以下の通りである。

① 暦年で少なくとも 180 日間マレーシアに物理的に滞在している者、又はマレーシア当局が容易に連絡を取れる者であること

② 当該個人はマレー語（Bahasa Malaysia）及び英語の双方に堪能であること

③ PDPA に関する十分な理解を有していること

DPO は、当該企業の既存従業員の中から選任することも、外部のサービス提供者から任命することも可能である。ただし、当該者は DPO としての職務と利益相反となる可能性のある責任を負ってはならず、組織の上級管理職に直接報告する体制としなければならない。

(3) DPO 選任時の通知義務

データ保護責任者（DPO）の任命にあたっては、任命日から 21 日以内に、正式な登録ポータルを通じて個人情報保護委員（Commissioner）に通知しなければならない。また、DPO 専用の電子メールアドレスを新たに作成し、割り当てる必要がある。この業務用メールアドレスは、当該個人の私用メールアドレスやその他の業務用メールアドレスとは明確に区別されていなければならない。

任命された個人またはその連絡先に変更が生じた場合には、当該変更から 14 日以内に Commissioner へ報告しなければならない。任命された DPO が辞任する場合や契約が終了する場合には、企業は速やかに後任者を任命するか、少なくとも、規制当局またはデータ主体からの照会に対応できる暫定的な担当者を指名しなければならない。

(4) DPO の責務

DPO の責務としては、PDPA に基づく義務について組織に助言を行い、内部のデータ保護方針の遵守状況を監視し、データ保護影響評価（DPIA）の実施またはその支援を行うほか、個人情報保護委員および影響を受けるデータ主体との正式な連絡窓口としての役割を担うことが求められる。また、DPO は、データ漏えい事案が発生した際には、その対応を監督する上で積極的な役割を果たすとともに、必要に応じて関連報告書の作成および Commissioner への文書提出を行わなければならない。

3. データ漏えいに関する通知義務

(1) 通知対象となる漏えい等

2025 年 6 月 1 日より施行される新制度の下では、データ管理者（Data Controller）は、個人情報の漏えい等が発生し、又は発生するおそれがあり、かつ、影響を受ける個人に重大な損害を与える場合には、個人情報保護委員（Commissioner）に対して当該漏えい事案を通知することが義務付けられる。

ただし、データ漏えい通知義務についても、DPO 選任義務と同様、あらゆる漏えい等が対象となるわけではない。

まず、通知の対象となる事象は、「データ侵害（Data Breach）」と広範に定義されており、人為的なミス、システム障害、又は悪意ある行為に起因する、個人情報への不正アクセス、不正開示、改ざん、又は破壊などの事案がこれに該当し、いわゆる情報漏えい事案以外も広く通知対象となる点に注意が必要である。

そして、このデータ侵害が、データ主体に対し「重大な損害」をもたらす結果となった、又はそのおそれがあると判断されるときに、可能な限り速やかに、かつ、漏えいを認知してから 72 時間以内に、個人情報保護委員（Commissioner）に対して通知しなければならないとされた。ここでいう「重大な損害（significant harm）」につき、ガイドラインは、以下の状況を挙げている。

- **身体的損害**：医療情報や健康情報の不正な開示など、個人の身体的安全を危険にさらす、又は身体的損傷を引き起こすおそれがある場合。
- **経済的損失**：銀行口座情報、決済情報、ログイン情報等の漏えいにより、詐欺的取引に悪用されるなど、実際の又は潜在的な経済的損害が発生するおそれがある場合。
- **信用情報への悪影響**：信用スコアや信用力に影響を与えるような信用関連データへの不正アクセスが行われた場合。
- **財産の損壊又は喪失**：アクセス認証情報や位置情報の漏えいにより、個人又は組織の資産の盗難や破壊を招くおそれがある場合。
- **違法目的での使用**：漏えいしたデータが、なりすまし、詐欺、恐喝、又はマレーシア国内外の法令に違反する活動に使用されるおそれがある場合。
- **機微な個人情報の関与**：漏えいに健康情報、財務状況、宗教的信条、政治的意見、犯罪歴等、PDPA 上「機微な個人情報」とされる情報が含まれる場合。
- **組み合わせによりなりすましが可能なデータ**：氏名、識別番号、連絡先情報などが組み合わされて漏えいし、当該データ主体になりすますために使用され得る場合。
- **大規模な影響**：1,000 人を超えるデータ主体に影響を与える漏えいである場合。この場合、個々の被害内容にかかわらず、規模の面から「重大」と見なされ、通知義務が発生する。

(2) 当局への通知に記載すべき事項

通知には、漏えいが発生した日時、漏えいの内容、影響を受けたデータの種類及び量、影響を受けた個人の人数、原因の疑い、及び封じ込めのために講じた措置など、特定の情報を含めなければならない。72 時間以内にすべての情報を提出することが困難な場合には、初期通知の後、30 日以内に段階的に追加情報を提出することが認められる。

なお、当該漏えいに複数のデータ管理者が関与している場合には、それぞれの管理者が個別に Commissioner へ報告を行わなければならない。

(3) データ主体への通知および記載すべき事項

データ管理者は、個人情報の漏えいが重大な損害を引き起こすおそれがある場合には、個人情報保護委員への通知に加え、影響を受けるデータ主体にも通知を行わなければならない。

この通知は、正当な理由なく遅延することなく行う必要があり、いかなる場合でも、個人情報保護委員への初期報告から 7 日以内に完了しなければならない。

データ主体への通知には、漏えいの内容、想定される影響、影響を軽減するために講じた措置、及び組織のデータ保護責任者（DPO）の連絡先情報を明確に記載しなければならない。通知は、電子メール、SMS、郵便などの直接的な手段により行う必要がある。ただし、連絡先情報が古い場合や、影響を受ける個人の数が非常に多い場合など、直接通知が非現実的であるときは、企業のウェブサイト、ソーシャルメディア、新聞等の公的手段を通じた公表によって通知を行うことができる。

(4) 通知に関する記録の保管

PDPA は、すべてのデータ漏えい及びその通知に関する記録を最低 2 年間保存し、要請があった場合には個人情報保護委員に提出できる状態にしておくことを企業に義務付けている。

(5) 罰則

通知義務に違反した場合、最大で 25 万リンギットの罰金、最長 2 年の懲役、又はその両方が科される可能性がある。

4. 2025 年 6 月 1 日までに講ずべき準備措置

施行日までに法令遵守を確保するため、マレーシアの個人情報を取り扱う外国企業は、以下の措置を講じる必要がある。

(1) DPO 選任義務の存否確認

自社がデータ保護責任者（DPO）の任命義務の基準を満たしているかどうかを判断するため、詳細な評価を実施しなければならない。任命義務が適用される場合には、適格な候補者の選定及び受け入れ、DPO 専用の業務用連絡チャネルの整備および所定の期間内に個人情報保護委員への登録手続きを完了することが求められる。

(2) データ漏えい通知に対応できる体制の確認

データ漏えい対応方針を見直し、PDPA の新たな通知義務に整合した具体的な手続を含める必要がある。これには、明確な社内報告ルート、文書管理手順、リスク評価基準、及び 72 時間及び 7 日以内の通知期限に対応できる体制の整備が含まれる。また、第三者データ処理業者との契約についても、迅速な漏えい報告及び協力義務に関する条項が盛り込まれていることを確認すべきである。

(3) 社内研修、社内資料の見直しなど

第三に、社内のデータ保護ガバナンスを強化するため、個人情報の取扱い、情報セキュリティ及びコンプライアンスに関与する従業員に対して、新たな法的義務に関する適切な研修を実施しなければならない。また、プライバシー通知、社内規程及び外部向け資料についても、DPO の任命及び漏えい対応手続を反映するよう更新する必要がある。

5. むすび

弊所では、DPO への就任、PDPA に関する社内研修の実施等、企業が適切な個人情報保護体制を構築するサポートを提供しております。本原稿に関するご質問などがございましたら何なりとお問い合わせ頂けますと幸いです。

◆ One Asia Lawyers ◆

「One Asia Lawyers Group は、アジア全域に展開する日本のクライアントにシームレスで包括的なリーガルアドバイスを提供するために設立された、独立した法律事務所のネットワークです。One Asia Lawyers Group は、日本・ASEAN・南アジア・オセアニア各国にメンバーファームを有し、各国の法律のスペシャリストで構成され、これら各地域に根差したプラクティカルで、シームレスなリーガルサービスを提供しております。

この記事に関するお問い合わせは、ホームページ https://oneasia.legal または info@oneasia.legal までお願いします。

なお、本ニュースレターは、一般的な情報を提供することを目的としたものであり、当グループ・メンバーファームの法的アドバイスを構成するものではなく、また見解に亘る部分は執筆者の個人的見解であり当グループ・メンバーファームの見解ではございません。一般的情報としての性質上、法令の条文や出典の引用を意図的に省略している場合があります。個別具体的事案に係る問題については、必ず各メンバーファーム・弁護士にご相談ください。

<著者>

橋本　有輝
One Asia Lawyers Group　マレーシアオフィス
弁護士（日本）

2005 年神戸大学法学部卒業、2008 年関西学院大学法科大学院修了、同年司法試験合格、その後日本で独立し、3 つの事務所を持つ法律事務所の代表弁護士を務める。建設業、不動産管理業、システム開発業、地方自治体、政党等、幅広い業種の顧問を務める。主な分野は、商業・企業アドバイザリー業務、不動産処分・買収、技術ベースの契約交渉など多岐にわたる。ワンアジア・ロイヤーズに入所後は、主に一般的な企業法務、ジョイント・ベンチャー、M&A、事業譲渡、株式資本の再編、海外投資、規制遵守、コーポレート・ガバナンス、雇用法、労働法関連のクロスボーダー取引の構築と処理に注力している。

yuki.hashimoto@oneasia.legal

Heng Zhenhung(Zed)
One Asia Lawyers Group　マレーシアオフィス
Paralegal（マレーシア）

2018 年に法学士号を取得し、2020 年にイングランド＆ウェールズの弁護士となる。
マレーシアに戻る前は、ロンドンを拠点とする慈善団体に勤務し、社会保障審判事件における法的助言、事件準備、弁護活動を行っていた。在職中は、雇用審判事件も担当した。
OAL 入社以前は、クアラルンプールにある法律事務所の税務リーガルチームに所属し、移転価格、税務、SST&GST、税関の案件を担当。OAL 入所後は、規制遵守、雇用法、契約法、土地法に関するサービスを提供している。

zhenhung.heng@oneasia.legal