マレーシア個人情報保護法の DPO 選任及びデータ侵害通知に関するガイドラインの解説

アジア & データ保護ニューズレター　　2025 年 4 月 4 日号

執筆者:
村田 知信
to.murata@nishimura.com
秋山 栞
s.akiyama@nishimura.com

マレーシアでは、2025 年 1 月 1 日から個人情報保護法（以下「**PDPA**」といいます。）の改正法が徐々に施行されており、同年 4 月 1 日には域外移転規制等に関する改正部分が施行され、同年 6 月 1 日にはデータ保護責任者（以下「**DPO**」といいます。）選任義務やデータ侵害通知に関する改正部分等が施行されます。また、これらの改正法の施行に伴い、関連するガイドラインも徐々に制定されてきています。

これらのガイドラインのうち、2025 年 2 月 25 日個人データ保護コミッショナー（以下「**コミッショナー**」といいます。）が公表した下記のガイドラインについては、実務への影響が特に大きいと思われます。

(a) DPO 選任に関するガイドライン（以下「**DPO ガイドライン**」といいます。）
(b) データ侵害通知に関するガイドライン（以下「**DBN ガイドライン**」といいます。）

本ニューズレターでは、上記ガイドラインの概要を解説します。なお、これらのガイドラインは、改正法の該当部分が施行される 2025 年 6 月 1 日から施行されます。

1. DPO ガイドライン

改正法により新設された PDPA の第 12 条 A は、一定の要件を満たすデータ管理者及びデータ処理者に対して DPO を選任する義務を課しています。DPO ガイドラインは、当該義務に関して概要以下を定めています。

	項　　目	概　　要
1.	DPO の選任要件	データ管理者及びデータ処理者は、個人データの処理に次の事項が 1 つ以上含まれる場合、1 人以上の DPO を任命する必要があります。 (a) データ主体が **20,000 人**を超える場合 (b) **10,000 人**を超えるデータ主体について、財務情報データを含む機密性の高い個人データを扱っている場合 (c) ターゲティング広告の目的でデータ主体がオンライン又はオフラインで追跡及びプロファイリングされるような、**個人データの定期的かつ体系的な監視を伴う場合**

2.	DPO の資格	データ管理者及びデータ処理者は、任命された DPO が以下のスキル、資質及び専門知識を十分なレベルで備えていることを確認する必要があります。 (a) PDPA 及びマレーシアのデータ保護慣行についての知識 (b) データ管理者/処理者のビジネス及び個人データ処理業務に関する理解 (c) 情報技術とデータセキュリティの理解 (d) 誠実さ、コーポレートガバナンスの理解、高い専門倫理などの個人的な資質 (e) 組織内でデータ保護文化を促進する能力
3.	DPO の候補	DPO は、自社の従業員から選任することも、サービス契約に基づいて外部者から選任することもできます。 DPO が契約を通じて選任された場合、データ管理者又はデータ処理者は、安定性を確保するために、少なくとも 2 年間は当該 DPO を選任し続けることが望ましいです。
4.	DPO 選任に関する通知	データ管理者は、DPO 選任から 21 日以内に、コミッショナーによって開設されている個人データ保護システムを通じて、DPO の氏名及びビジネス連絡先情報をコミッショナーに通知する必要があります。また、通知した情報に変更がある場合、14 日以内に当該システムを通じて情報を更新する必要があります。
5.	DPO の任務及び責任	DPO は、データ管理者又はデータ処理者のデータ処理活動に関して、少なくとも以下の責任を負います。 (a) 個人データ処理についてデータ管理者/処理者に情報やアドバイスを提供すること (b) PDPA 及び関連法の遵守に関するサポート（データ管理者/処理者に影響を与えるデータ処理リスクに関する情報を常に把握することを含む） (c) コミッショナーが随時決定する可能性のある要件に従ってデータ保護影響評価を実施すること (d) データ管理者/処理者の個人データ法令順守を監視すること (e) 個人データ侵害に関してコミッショナーが必要とするレポート及びその他の文書の準備、処理、提出を支援することにより、データ侵害及びセキュリティインシデントについて適切な対応を行うこと (f) その他、コミッショナー又はデータ管理者/処理者が随時要求する責任 データ管理者/処理者は、DPO が十分な独立性と自律性を持って

		職務を遂行するために必要なリソースが提供されていることを確認する必要があります。さらに、DPO は、データ管理者/処理者の上級管理職に直接報告ができる必要があります。
6.	利益相反	DPO は、他の業務を遂行することができますが、データ管理者/処理者は、**そのような他の業務の遂行が DPO に利益相反を引き起こさないようにするもの**とします。
7.	アクセシビリティ	DPO は、DPO のサービスを受ける者が DPO に簡単にアクセスできることを確保する必要があります。 そのために、DPO は、(a)マレーシアに居住している（1 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）か、何らかの手段で簡単に連絡できる必要があり、(b)**マレー語と英語に堪能であることも必要です**。

DPOガイドラインによって明らかになったマレーシアのDPO選任義務の建付は、①選任義務が発生するハードルが高く、かつ、②選任義務が発生した場合適切な候補者を発見するハードルも高いものとなっています。

①について、機密性の高い個人データを処理していても、データ主体の人数が 10,000 人を超えないと選任義務が発生しないため、例えばメーカーの現地拠点が従業員や取引先従業員の個人データを処理しているだけであれば、選任義務を負うことは珍しいと思われます。ただ、ターゲティング広告等の目的で個人データの定期的かつ体系的な監視を伴う場合には選任が必要となり得るため、特に B to C ビジネスを行っている場合は留意が必要です。

②について特筆すべきは、**利益相反禁止とマレー語及び英語能力があることが明示的に要件となっている**ことです。東南アジアでは、日系企業の現地拠点が DPO を選任する場合、現地拠点代表の日本人駐在員を選任するような事例が多いですが（特にシンガポールやベトナムのように DPO 選任義務が発生するハードルが低く候補者の要件も厳しくない国で多く見られます）、上記要件を踏まえると、マレーシアでは、多くの日系企業でそのような方針を採ることは難しくなりそうです。上記要件を満たすために、**マレー語能力があるマレーシア人専門家を社内で育成する又は委託先として起用することで DPO 選任義務に対応せざるを得ない事例が増えてくる**ように思われます。

2. DBN ガイドライン

改正法により新設された PDPA の第 12 条 B は、データ管理者に対して、コミッショナーと影響を受けるデータ主体の両方に個人データ侵害を通知する義務を課しています。DBN ガイドラインは、当該義務に関して概要以下を定めています。

	項　　目	コミッショナーへの通知	影響を受けるデータ主体への通知
1.	データ侵害通知	データ管理者は、個人データ侵害が	データ管理者は、個人データ侵害が

	義務が発生する要件	「重大な損害」を引き起こす又は引き起こす可能性がある場合、具体的には侵害された個人データについて以下のリスクがある場合、コミッショナーに通知する必要があります。 (a) 身体的危害、経済的損失、信用記録への悪影響、又は財産の損害又は損失につながる可能性がある場合 (b) **違法な目的で悪用される可能性がある場合** (c) 機密性の高い個人データで構成されている場合 (d) 個人データとその他の個人に関する情報で構成されており、これらが組み合わさると、**なりすましを可能にする場合** (e) 影響を受けるデータ主体の数が**1,000 人**を超える場合	「重大な損害」を引き起こす又は引き起こす可能性がある場合、影響を受けるデータ主体に通知する必要があります。基本的にはコミッショナーへの通知と同様の枠組みで判断されますが、左記(e)の要件は除外されます。
2.	通知のタイムライン	通知は、可及的速やかに、個人データ侵害の発生から 72 時間以内に行われるものとします。 データ管理者が 72 時間以内に通知しなかった場合、インシデントのタイムライン、内部コミュニケーション、遅延の原因となった関連要因等について、裏付けとなる証拠を添えた書面によりコミッショナーに対して説明をする必要があります。	影響を受けるデータ主体への通知は、最初のデータ侵害通知がコミッショナーに対して行われてから 7 日以内に、不必要な遅延なく行う必要があります。
3.	通知の手続き及び形式	コミッショナーへの通知は、次のいずれかのチャネルを通じて行われる必要があります。 (a) コミッショナーの公式ウェブサイトに掲載されている通知フォームに記入する。 (b) DBN ガイドラインの付録 B に掲載されている通知フォームをコミッショナーの電子メールアド	影響を受けるデータ主体への通知は、データ主体が侵害の可能性のある影響から身を守るために必要な予防措置又はその他の措置を講じることができるように、状況に適したわかりやすい言語を使用して、直接かつ個別に実施される必要があります。 直接の通知が実行不可能であるか、又は過分なコストが必要な場合、データ

		レス宛に送付するか又はハードコピーをコミッショナーに提出する。	管理者は、代替の通知手段を使用することができます。
4.	対応計画の策定	データ管理者は、適切なデータ侵害への対応計画を策定する必要があります。このような計画には、少なくとも、(a)個人データ侵害の特定に関する手順、(b)関連する利害関係者の役割と責任、(c)侵害の影響を軽減するための手順、を織り込む必要があります。	
5.	データ処理者との契約に規定すべき義務	データ管理者は、発生したデータ侵害についてデータ処理者から迅速に報告を受け、PDPA に基づくデータ管理者のデータ侵害通知義務を果たすために、データ管理者に合理的かつ必要な支援を提供する義務をデータ処理者に契約上課すことが義務付けられています。	
6.	個人データ侵害の記録を保持する義務	データ管理者は、コミッショナーへの通知日から少なくとも 2 年間、コミッショナー及び/又は影響を受けるデータ主体に通知するための通知基準を満たさなかったものを含め、個人データ侵害の記録を保持するものとします。	

DBN ガイドラインによって明らかになったマレーシアのデータ侵害通知義務の建付は、「重大な侵害」を引き起こす可能性を通知義務発生の要件としており、データ主体の人数で見ると 1,000 人が基準であることが明確にされていることから、自社従業員の過失によるセンシティブ性が高くない個人データのデータ侵害等（メール誤送信等）の場合には、通知が不要と整理可能な場合も多いように思われます。もっとも、**個人データが違法な目的で悪用される可能性がある場合や、なりすましを可能にする場合は人数が少人数でも通知が必要とされていることから、ランサムウェア等のサイバー攻撃によってデータ侵害が発生した場合には、通知が必要となることが多いように思われる**ため、注意が必要です。

西村あさひ 広報課 newsletter@nishimura.com