西村あさひ法律事務所

バーレーンにおける個人データ保護法(2)

中東ニューズレター 2023 年 1 月 16 日号

執筆者:
E-mail 森下 真生 E-mail 中島 朋子

1. バーレーンにおける個人データ保護法

前回(バーレーンにおける個人データ保護法(1))紹介したとおり [1]、バーレーンにおいては、2019 年 8 月 1 日から、包括的な個人データ保護に関する法律として全 60 条から成る個人データ保護法(Personal Data Protection Law)(以下、「PDPL」と言います。)が施行されており、また、2022 年 3 月 17 日には、PDPL の下位ルールとして合計 10 種類の指令(Order)が定められています。

本ニューズレターでは、前回に続き、PDPL 上のデータ管理者の義務、及びデータ主体の権利について解説します。

2. データ管理者の義務

(1) 個人データ保護のための技術的及び組織的措置の実施

データ管理者は、個人データの保護のための技術的及び組織的措置の実施を求められます。

具体的には、データ管理者は、偶発的又は権限なくなされるデータの破壊、偶発的なデータの逸失、改ざん又は開示、アクセス及びその他のあらゆる不正な形式の処理に対するデータの保護を確保するために、適切な技術的及び組織的対策を実施しなければならず、その対策は、最新の技術的なセキュリティ対策、関連コスト、処理されるデータの性質及びリスクの可能性を考慮して、適切なレベルの安全性を提供することを確保するものでなければなりません。加えて、技術的及び組織的な対策は記録され、全ての関係者、個人データ保護当局及びデータ処理者がアクセスできる必要があります(PDPL8 条 1 項。以下、法令名の記載のない条文番号については、PDPL の条文番号を指します。)。また、データ管理者は、適切な安全性を確保するために、個人データを処理する際に、処理の範囲、状況、目的又はリスクに応じて、以下の技術的及び組織的対策の全部又は一部を実施する必要があります(指令 2022 年 43 号 2 条)。

① データの処理に使用されるアプリケーション、サービス及び製品を準備、設計、選択又は使用する際に、プライバシー・バイ・デザイン(Privacy by Design)を実施すること
② PDPL 及び指令に従い、個人データの保護に関連する仕組み、実務慣行及び指示を通じて、プライバシーフレームワークを確立すること
③ 違反に対処するための効果的な対策及び違反のリスクの軽減を目的とした対応をすること(保存されたデータへのアクセス規制、パスワードの保護、ウィルス対策ソフトウェア及びファイアーウォールの使用、ソフトウェアライセンスの遵守、データの保持及び廃棄期間の規定、データバックアップ対策の規定、適切な技術開発、物理的・仮想的に維持されるデータのアクセス制御及びセキュリティの確保など)
④ 脆弱性診断及び侵入テスト(Vulnerability Assessment and Penetration Testing:VAPT)を定期的に実施し、実行されたセキュリティ対策の効率を検証・測定し、セキュリティの脆弱性を修正及び軽減すること
⑤ データ処理システムへの突然の侵害に対処するための効果的な計画を策定し、中断なく処理を継続できるようにすること
⑥ 処理されたデータの高度な保護及びプライバシーを確保するため、タスクに応じた適格な従業員を割り当てること

[1] 2022 年 12 月 1 日付のニューズレターをご参照ください。

© Nishimura & Asahi 2023

(2) データ処理者の選任・監督

データ管理者は、データ処理に際してデータ処理者を選任する場合、必要な技術的及び組織的な措置の実施に関して十分な保護措置を講じうるデータ処理者を選任しなければならず、処理が、データ管理者とデータ処理者の間の書面による契約に従って行われることを確保しなければなりません(8 条 3 項)。

(3) 個人データの開示の禁止等

データ管理者は、個人データ保護主体の同意がある場合又は管轄裁判所、検察、捜査判事、若しくは軍検察が発する命令に従う場合を除き、個人データを開示することはできません(9 条 1 項)。また、データ管理者は、PDPL に反して個人データを処理してはならず、かかる禁止義務は、雇用関係又は契約期間の終了後も同様に課されます(9 条 2 項)。なお、いかなる場合も、個人データにアクセスできる個人は、データ管理者の同意又は管轄裁判所等の命令なく、個人データの処理を行うことは禁止され、個人的又は他人の利益のために個人データを使用することはできません(同項)。

(4) 当局に対する個人データ保護監督者の選任通知

PDPL 上、データ管理者は、外部又は内部のデータ保護監督者(Data Protection Guardian)を選任することができるとされ、選任した場合には 3 営業日以内に、個人データ保護当局に通知する必要があります(10 条 4 項、指令 2022 年 46 号 2 条)。データ保護監督者は以下の責任を負います(10 条 1 項)。なお、データ保護監督者は、EU の一般データ保護規則(General Data Protection Regulation)(以下、「GDPR」と言います。)におけるデータ保護オフィサー(Data Protection Officer)に類似しますが、一定の場合に選任が義務となる GDPR におけるデータ保護オフィサーの場合と異なり、PDPL 上、データ管理者にデータ保護監督者の選任を義務付ける条項はありません。

① PDPL に基づくデータ管理者の権利行使及び義務遵守のサポート
② 個人データの処理に関連する特定の規定の管理者による実施に際する、個人データ保護当局とデータ管理者の間の調整
③ データ管理者によるPDPLに従った個人データの処理の確保(個人データ保護監督者が違反を把握した場合、直ちにデータ管理者に注意喚起し、違反の原因を明らかにし、可及的すみやかに必要な是正を行わなければなりません。)。
④ データ管理者が 10 日を経過しても違反の是正・排除を行わない場合、当該違反に関する新しい証拠を取得した際の個人データ保護当局への通知
⑤ PDPL 14 条(後記⑸参照)に従い、データ管理者が個人データ保護当局に通知する義務を負う処理に関する記録の保管
⑥ 独立且つ公平な職務遂行

データ保護監督者は、データ処理者登録局(Data Protection Controller Registry)に登録される必要があります(指令 2022 年 46 号 4 条)が、指令 2022 年 46 号は、その登録にあたり充足する必要のあるデータ保護監督者の適格性に関する要件を定めており(同 5 条、9 条)、データ保護監督者として選任される者は、その要件を充足する必要があります。たとえば、内部のデータ保護監督者の場合には、データ管理者又はそのグループ会社等の従業員であり、バーレーンの居住者であることが求められます(同 9 条)。

(5) 自動化された処理に関する当局への通知

データ管理者は、一定の例外を除き、ひとつの目的又は複数の関連する目的のために、個人データの一部又は全部の自動化された処理(PDPL 上の「処理」は、収集も含む語として定義されています。)を行う場合、事前に、個人データ保護当局に対し、以下の事項を書面で通知する必要があります(14 条 1 項、2 項、指令 2022 年 44 号 2 条)。通知に関する詳細は、指令 2022 年 44 号に定められています。

① データ管理者及びデータ処理者(選任されていれば)の氏名/名称及び住所
② データ処理の目的
③ 個人データの概要、データ主体のカテゴリー及び個人データの受領者又はそのカテゴリー
④ 予定されるバーレーン外の国及び地域へのデータの移転
⑤ 個人データ保護当局が、PDPL 8 条(前記 2.(1))に従った個人データ保護のための安全措置の妥当性に関する初期的評価ができるような説明

Ⓒ Nishimura & Asahi 2023

(6) データ主体への通知

データ管理者は、データ主体から個人データを取得する場合、データ主体に対し、PDPL に規定された情報を通知しなければなりません(17 条 1 項及び 2 項)。直接取得する場合の通知内容は以下のとおりです（同 1 項）。

① データ管理者の氏名/名称、活動分野又は専門領域(必要に応じて)、及び住所
② データ処理の目的
③ 以下を含む特定の状況を考慮してデータ主体にとってデータの公正な処理を確保するために必要な追加の情報
  (i) データ受領者の氏名/名称又はカテゴリー
  (ii) データ主体に対する質問への回答が必須か任意か、及び回答しない場合の結果
  (iii) データ主体が要求に応じて自身に関する完全なデータについて通知を受ける権利及びその修正を要求する権利
  (iv) 個人データがダイレクトマーケティング目的で使用されるか否か
  (v) データ主体が PDPL に基づいて自らの権利を追及することを可能にするその他の情報

また、データ管理者は、データ主体の請求に基づき、費用を徴収することなく、請求を受けた日から 15 営業日以内に、当該データ主体の個人データが処理されているか否か、及び、処理されている場合には以下の情報を通知しなければならないとされます(18 条)。

① 処理対象の全ての個人データ
② 法律上守秘義務を負う場合を除く、データ管理者において把握可能な収集源に関する全ての情報
③ 個人データの処理目的
④ データ受領者の氏名又はカテゴリー
⑤ データが、データ主体の個人的な利益に直接的に影響を及ぼす決定を行う唯一の根拠である場合、データの使用方法

(7) センシティブ情報の取り扱い

センシティブ情報を取り扱う場合、データ管理者には、さらに以下の義務が課されます(5 条、指令 2022 年 45 号 4 条)。

① 処理は、許可された範囲且つデータ主体の同意の範囲内、又は当局によってなされた許可の範囲内で実行されなければならず、いかなる場合でも、センシティブ情報を他の目的で処理しないこと
② 指令 2022 年 43 号に従い、違法な処理及びプライバシーの侵害に対する保護を確保し、データの損傷、損失、漏洩、複製を防止する高レベルの安全性を備えた技術的対策を行うこと
③ データ主体の同意の上で指定された期間、当局による許可によって指定された期間、又はデータ管理者の活動が服する規則等に規定された期間を超えて、データを保持しないこと

3. データ主体の権利

PDPL 上、データ主体には、以下の権利が認められます。他方、GDPR のデータポータビリティ権に対応する権利に関する規定はありません。

(1) 同意権及び同意の撤回権

データ主体は、個人データの処理について同意を行う権利を有し(4 条)、当該同意について、撤回前に行われた処理を害しない限度で、撤回する権利を有します(24 条 3 項、指令 2022 年 48 号 6 条)。

(2) 通知を受ける権利及びアクセス権

前記 2.(6)のとおり、データ主体は、データ管理者から、データ管理者の情報、データ処理の目的、データの公正な処理のために必要な情報について、通知を受けることができます(17 条 1 項及び 2 項)。また、データ主体は、データ管理者に対し、個人データが処理されているか否かの確認を求めることができ、処理されている場合には、処理対象の全ての個人データ、データの収集源、データの処理目的、データ受領者の情報等の事項の通知を受けることができます(18 条 1 項)。これらは、GDPR における情報権(13 条及び 14 条)とアクセス権(15 条)に類似する内容です。

© Nishimura & Asahi 2023

(3) ダイレクトマーケティングに関する権利

データ管理者が、法律上公開が義務づけられている個人データを含め、保有する個人データがダイレクトマーケティングの目的で処理される可能性があると認めた場合、データ管理者はデータ主体にその旨を通知する必要があり、データ主体に当該処理に対し異議を述べる機会を与える必要があります(19 条)。データ管理者は、データ主体から身分を証明した上で当該処理を行わないことを要求された場合、要求を受けてから 10 営業日以内に、ダイレクトマーケティング目的での処理を開始しないか、又は中断する必要があります(20 条 1 項)。この規定は、GDPR のダイレクトマーケティングに対する規制(GDPR 21 条 2 項乃至 4 項)に類似する内容です。

(4) データ処理の中止に関する権利

データ管理者は、例外的な場合を除き、以下の場合においては、データ主体が、理由とその証拠と共に、身分を証明した上で要求した場合、当該要求を受けてから 10 営業日以内に、当該データ主体に関する個人データの処理の開始をとりやめ、又は個人データの処理を全体的に、若しくは特定の目的のため若しくは特定の方法において、中止しなければなりません(21 条)。

① 当該目的又は当該方法による個人データの処理が、個人データ主体又は別の主体に対して、物質的又は精神的な不当で重大な損害を引き起こしている場合。
② 当該目的又は当該方法による個人データの処理が、個人データ主体又は別の主体に対して、物質的又は精神的な不当で重大な損害を引き起こす合理的な可能性がある場合。

(5) 自動処理のみによる決定の対象とならない権利

個人データの自動処理に関する決定が、データ主体の勤務成績、財務状態、信用度又は信頼性に関してデータ主体を評価することを目的とする場合、データ主体は、自動化されていない方法による処理を要求する権利を有し、この場合、決定を行った者には無償での再検討が義務づけられます(22 条 1 項)。もっとも、データ主体の正当な利益を保護するための適切な措置が講じられていることを条件として、データ主体とデータ管理者との間の契約の締結又は履行に必要な場合には、自動処理のみによる決定も許されるとされます(22 条 2 項)。これは GDPR のプロファイリングを含む個人に対する自動化された意思決定に関する規定(GDPR 22 条)に対応した規定と考えられます。

(6) 個人データ修正、ブロック及び削除権

データ主体は、PDPL に反する場合、とりわけ、データが不正確、不完全若しくは古い場合、又はデータ処理が不法に行われた場合、データ管理者に対して、身分を証明した上で、個人データの修正、ブロック、又は削除を要求する権利を有します。データ管理者は、当該要求が法的に正当化しうる場合、費用を徴収することなく、要求を受けてから 10 営業日以内に対応を行う必要があります(23 条 1 項)。これらの権利は、GDPR の個人データ訂正権(GDPR 16 条)及び削除権(GDPR 17 条 1 項)に類似する権利と言えます。

(7) 不服申立権

データ主体は、自らの個人データの処理が PDPL に準拠していないと考える場合、指令 2022 年 49 号の定めに従い、所定のフォームを利用して必要事項を記載した上で、個人データ保護当局に不服を申し立てることが可能です(25 条、指令 2022 年 49 号 2 条及び 3 条)。

Ⓒ Nishimura & Asahi 2023

中東関連イベント情報

UAE ウェブ法律相談
当事務所によるウェブを通じた日本語無料法律相談(30 分程度)を実施いたします。ご希望者は、ご相談事項を明記の上、こちらまでご連絡ください。

トルコウェブ法律相談
当事務所とトルコの現地法律事務所によるウェブを通じた無料法律相談会(30 分程度)を実施いたします。現地法律事務所とのやり取りは英語になりますが、当事務所により、回答可能な場合は、日本語で対応いたします。また、事前に当事務所弁護士との日本語での準備面談も可能です。ご希望者は、ご相談事項を明記の上、こちらまでご連絡ください。

その他中近東各国ウェブ法律相談(バーレーン、カタール、イスラエル、エジプト)
当事務所と各国現地法律事務所によるウェブを通じた無料法律相談会(30 分程度)を実施いたします。現地法律事務所とのやり取りは英語になりますが、当事務所のみにより、回答可能な場合は、日本語で対応いたします。また、事前に当事務所弁護士との日本語での準備面談も可能です。ご希望者は、ご相談事項を明記の上、こちらまでご連絡ください。

イスラエル事業環境個別ウェビナー
イスラエル法律事務所によるウェブを通じたイスラエル事業環境に関する無償プレゼンテーション(30 分から 1 時間程度)を実施いたします。現地法律事務所とのやり取りは英語になりますが、当事務所にて適宜日本語の補足を行うことは可能です。ご希望者は、こちらまでご連絡ください。

当事務所では、クライアントの皆様のビジネスニーズに即応すべく、弁護士等が各分野で時宜にかなったトピックを解説したニューズレターを執筆し、随時発行しております。N&A ニューズレター購読をご希望の方は N&A ニューズレター　配信申込・変更フォームよりお手続きをお願いいたします。
また、バックナンバーはこちらに掲載しておりますので、あわせてご覧ください。

本ニューズレターはリーガルアドバイスを目的とするものではなく、個別の案件については当該案件の個別の状況に応じ、日本法または現地法弁護士の適切なアドバイスを求めていただく必要があります。また、本稿に記載の見解は執筆担当者の個人的見解であり、当事務所または当事務所のクライアントの見解ではありません。

西村あさひ法律事務所　広報室　E-mail

Ⓒ Nishimura & Asahi 2023