

執筆者:

E-mail☒ [村田 知信](mailto:chikuda@nishimura-asahi.com)E-mail☒ [イカング・ダーヤント](mailto:ikang@nishimura-asahi.com)E-mail☒ [マデ・グラジア・バリアナ・ウストリヤナ](mailto:mada@nishimura-asahi.com)

インドネシアには長年包括的な個人データ保護法が存在せず、電子システムの利用等を規制する個別法に関連する規制が存在するのみであったが、2022年10月17日に遂に個人データ保護法(Law No. 27 of 2022 on Personal Data Protection)(以下「PDP法」という。)が制定・施行された。同法には2年間の猶予期間が設けられているため、インドネシアで事業を行っている企業は、2024年10月17日までに同法を遵守するための法令対応作業を実施する必要がある。

PDP法は、多くの点でEUのGDPR(General Data Protection Regulation)と類似した建付を採用しているため、PDP法の法令対応作業は、基本的にはGDPRの法令対応作業と同様の手順を進めることができると考えられる。そのため、既にグループ内の欧州拠点や日本本社においてGDPR対応を実施済みの企業については、基本的にはGDPR対応の際の方法を踏襲するのが効率的だと思われる。ただし、PDP法はGDPRの完全コピーというわけではなく、GDPRと異なる点も少なくない。そのため、GDPR対応をベースに法令対応作業を進める場合、PDP法の規制内容がGDPRとどのような点が同じでどのような点が異なるのか、正確に理解しておく必要がある。

PDP法の内容については、既に[アジアニュースレター2022年9月26日号「インドネシア初の個人情報保護法」](#)で法案段階の概要を紹介したが、本稿では、当該ニュースレター後に公布された法令の内容を踏まえて、今後PDP法の法令対応作業を実施する際に重要となる各論点について、より詳細に規制内容を説明する。

## 1. 個人データの定義

PDP法は、個人データを、「個人に関するデータであって、電子的又は非電子的方式により直接又は間接的に(個人が)識別され、又は他のデータと結び付いて識別され得るもの」と定義した上で、以下の特定個人データと一般個人データに分類している。

### a. 特定個人データ(以下が含まれると規定されている)

- 健康データ又は情報。例えば、身体的健康、精神的健康、及び/又は健康サービスに関連する個人の記録又は情報。
- バイオメトリクスデータ。例えば、顔画像又は指紋鑑定データのような個人のユニークな識別を可能にする個人の身体的、生理的又は行動的特徴に関連するデータ。バイオメトリクスデータは、指紋記録、目の網膜、DNAサンプル等の保護・維持しなければならない個人の固有性及び/又は特性を記述するものでなければならないが、これらに限定されない。
- 遺伝データ。例えば、出生前発達中に遺伝する又は獲得される個人の特性に関するあらゆる種類のデータ。
- 犯罪記録。例えば、違法又は不法な行為を行った人、又は犯した行為について裁判中の人に関する書面による記録であり、警察の記録や防止又は抑止リストへの掲載を含む。
- 子供のデータ。
- 個人の金融データ、例えば、クレジットカードや銀行での預金、振込等に関するデータ。
- 法令等が定めるその他のデータ。

b. 一般個人データ(以下が含まれると規定されている)

- 氏名
- 性別
- 国籍
- 宗教
- 配偶者の有無
- 携帯電話番号や IP アドレス等、組み合わせられ個人を特定する個人データ

上記のような一定の種類個人データを特別に定義する建付は、GDPR におけるセンシティブ個人データと類似している。もっとも、PDP 法における特別個人データの定義は、GDPR におけるセンシティブ個人データの定義内容とは異なる点がある(GDPR と異なり宗教に関するデータは特別個人データとされていない等)。

また、PDP 法では、GDPR のようなセンシティブ個人データの処理に原則データ主体の同意が必要とされる建付は採用されていない(すなわち処理のための適法性の根拠は他の個人データと同様に判断される)。特定個人データを処理するために追加で負い得る義務は、少なくとも法令文言上は、データ保護影響評価の実施義務と DPO 選任義務のみである(この点は下記 9 及び 10 で述べる)。

なお、PDP 法においても、子供の個人データの処理には法定代理人の同意が必要とされている。

## 2. 管理者及び処理者の区別

PDP 法では、GDPR と同じく、個人データを処理する主体を下記の管理者及び処理者に区別し、処理者には管理者に適用される義務の一部のみを適用する反面、管理者に対して処理者によるデータ処理の責任を負わせる建付が採用されている。

- a. 管理者: 個人データの処理の目的を決定し、管理権を行使するために自ら又は共同して行動する全ての個人・企業、公的機関及び国際機関。
- b. 処理者: 管理者に代わって個人データ処理において自ら又は共同して行動する全ての個人・企業、公的機関及び国際機関。

具体的には、①処理者は管理者の指示に基づいて個人データを処理しなければならない、②管理者は処理者による個人データの処理に責任を負う、③処理者は他の処理者に処理を委託する場合管理者から書面による承諾を受けなければならない等の義務が規定されている。

なお、PDP 法においては、少なくとも法令文言上は、GDPR と異なり、管理者が処理者と書面によるデータ処理契約(DPA)を締結する必要がある旨及びその内容は明確に規定されていない。しかし、上記のとおり、管理者は、自らの指示に従って処理者に個人データを処理させ当該処理に責任を負う必要があるため、処理者と契約を締結することでこれらの義務・責任を果たす必要があると考えられる。

## 3. 適用範囲及び域外適用

PDP 法は、個人データを処理する個人・企業、公的機関及び国際機関が以下の要件を満たす場合に適用される。

- a. インドネシア域内に所在する場合
- b. インドネシア域外に所在し、かつ、インドネシア域内に法的影響を及ぼす又はインドネシア域外に所在するインドネシア国民のデータ主体に法的影響を及ぼす場合

すなわち、PDP 法は上記 b の要件を満たす場合は日本等の外国に所在する管理者等にも域外適用されることになる。当該域

外適用の要件は、域内への商品・サービス提供や域内のデータ主体の監視を要件とする GDPR とは異なっており、法的影響とは何を意味するのか・どのようにその有無を判断するのかについては、法令文言上不明確である。なお、GDPR と異なり、PDP 法では、域外の管理者等に PDP 法が適用される場合であっても、域内の代理人の選任は求められていない。

また、PDP 法は、個人による個人的又は家事的な活動のための個人データの処理や以下の目的による個人データの処理にも適用されない。

- a. 国防・安全保障上の利益
- b. 法執行機関の利益
- c. 国家行政の文脈における公共の利益
- d. 金融サービス部門の監督、及び国家行政の文脈で行われる通貨、決済システム、金融システムの安定

#### 4. 個人データ処理の原則

PDP 法は、個人データを処理する際は以下の原則に従わなければならない旨定めている。

- a. 個人データの収集は、限定的、具体的かつ法的に有効で、透明性のあるものでなければならない。
- b. 個人データの処理は、その目的に従って行われるものとする。
- c. 個人データの処理は、データ主体の権利を保証して行われるものとする。
- d. 個人データの処理は、正確及び完全であり誤解を招かない最新かつ説明可能な方法で実施されるものとする。
- e. 個人データの処理は、不正アクセス、不正開示、改ざん、誤用、破壊、及び/又は紛失から個人データを保護して行われるものとする。
- f. 個人データの処理は、その目的、処理の活動、保護の失敗を通知して行われるものとする。
- g. 個人データは、法令に別段の定めがある場合を除き、保有期間終了後又はデータ主体の求めに応じて廃棄又は削除されるものとする。
- h. 個人データの処理は、責任を持って実施され、明確に説明可能である必要がある。

#### 5. 適法性の根拠

PDP 法では、個人データを処理するために以下のいずれかの適法性の根拠を満たすことが必要とされている。

- a. 同意: 通知された1つ又は複数の特定の目的に対するデータ主体からの明確かつ有効な同意
- b. 契約: データ主体が当事者である契約上の義務の履行又は契約締結時のデータ主体からの要求への対応
- c. 法的義務: 管理者の法的義務の履行
- d. 生命に関する利益: データ主体の生命に関する利益の保護
- e. 公的義務: 公益若しくは公共サービスにおける義務履行又は法令に基づく管理者の権限行使
- f. 正当な利益: 管理者の目的、必要性、管理者の利益とデータ主体の権利のバランスを考慮したその他の正当な利益

インドネシアでは、従前個人データの処理のためには原則データ主体の同意が必要とされてきたが、PDP 法では、少なくとも法令文言上は、GDPR と類似した適法性の根拠が規定され、データ主体の同意はあくまで適法性の根拠の1つとして整理された。また、GDPR と同じく正当な利益に基づくデータ処理も認められている。

#### 6. データ主体からの同意の取得方法

PDP 法は、データ主体からの同意は、大要、下記 7 の通知事項を通知した上で、書面その他記録に残る形で、インドネシア語でシンプルかつ理解し易い方法で取得される必要がある旨定めている。また、電子的な同意取得も可能だとされている。

言語が指定されているのが特徴的であるが、インドネシアにはそもそも言語法という法令が存在し、インドネシア法人が当事者

となる契約書は基本的にインドネシア語版の作成も要求されるため、インドネシアではある意味当然の要件であると思われる。

なお、同意の任意性についてどの程度厳しい解釈が採用されるのか(GDPR のように従業員からの同意取得について無効と解釈され得る可能性があるのか等)については、現状では指針がなく不明確である。

## 7. データ主体への通知事項

PDP 法では、管理者が個人データを処理するためには、事前に以下の事項をデータ主体に通知(情報提供)する必要があり、変更がある場合は変更前に当該変更について通知する必要がある。

- a. 処理の適法性根拠
- b. 処理の目的
- c. 処理される個人データの種類と関連性
- d. 個人データを含む文書の保管期間
- e. 収集される情報の詳細
- f. 個人データの処理期間
- g. データ主体の権利

全体的に、GDPR と比べて通知事項は少ないが、どのような内容を通知すればよいのか不明確な事項もあり、下位規則による明確化が望まれる。

## 8. データ主体の権利

PDP 法において、データ主体には自らの個人データについて大要以下の権利が認められている。ただし、PDP 法上一定の場合は管理者は下記の権利行使を拒否することができる。

- a. 個人データ処理に関して説明を受ける権利
- b. 不正確な個人データを訂正する権利
- c. 個人データにアクセスする権利
- d. 個人データの処理を中止させ削除する権利
- e. 同意を撤回する権利
- f. プロファイリングを含む自動処理のみに基づく意思決定行為で法的影響を及ぼすもの又はデータ主体に重大な影響を及ぼすものに対して異議を唱える権利
- g. 個人データの処理を遅延させる又は制限する権利
- h. 違法な個人データ処理について訴訟を提起して補償を受ける権利
- i. 一般的に使用されている又は電子システムで読み取り可能な構造・形式に従った形で個人データを入手・利用する権利
- j. 個人データを他の管理者に送信し利用させる権利

## 9. データ保護影響評価

PDP 法は、以下の場合を含む個人データの処理がデータ主体に高いリスクをもたらす可能性がある場合、管理者はデータ保護影響評価(Data Protection Impact Assessment)を実施しなければならないという、GDPR に類似した規制を導入している。

- a. データ主体に法的な影響又は重大な影響を与える自動的な意思決定
- b. 特定個人データの処理
- c. 大規模な個人データの処理
- d. データ主体の体系的な評価、採点又は監視のための個人データの処理
- e. データグループの照合又は結合のための個人データの処理

- f. 個人データの処理における新しい技術の使用
- g. データ主体の権利行使を制限する個人データの処理

## 10. データ保護責任者

PDP 法は、管理者及び処理者は以下の場合にデータ保護責任者(Data Protection Officer)を選任しなければならないという、GDPR に類似した規制を導入している。

- a. 個人データが公共サービスのためのものである場合
- b. 管理者の主要な活動が、大規模な個人データの定期的かつ体系的な監視を必要とする性質、範囲又は目的を有していること
- c. 管理者の主要な活動が、特定個人データ又は犯罪に関連する個人データの大規模な処理から構成されていること

データ保護責任者は、専門性、データ保護法に関する知識・実務経験・職務遂行能力に基づいて任命され(PDP 法には国籍、所在地、言語の要件は規定されていない)、管理者又は処理者が企業の場合、内部者から選任することも外部専門家を選任することも可能である。また、データ保護責任者は、少なくとも以下の任務を負うものとされている。

- a. PDP 法を遵守するために管理者又は処理者に情報や助言を提供すること
- b. 管理者又は処理者による PDP 法及びポリシーの遵守状況を監視し確認すること
- c. 個人データ保護影響評価及び管理者及び処理者によるその実施の監視に関する助言を提供すること
- d. 個人データの処理に関する問題をリエゾンとして調整すること

なお、インドネシアでは、PDP 法制定以前から、電子システムにおける個人データの保護に関する通信情報大臣 2016 年規則第 20 号に基づき、個人データの管理に関してデータ主体が容易に連絡できる窓口を提供することが求められており、当該義務は PDP 法制定後も有効である。

## 11. 国外移転

PDP 法は、個人データを国外に移転する管理者は、移転先の国が PDP 法と同等以上の個人データ保護水準を有することを確認しなければならないという要件を規定している。ただし、以下の場合には当該要件は適用されないとされている。

- a. 管理者が十分かつ拘束力のある個人データ保護を確保できる場合
- b. a.を満たすことができない場合、データ主体の同意があるとき

PDP 法は、移転先の国が PDP 法と同等以上の個人データ保護水準を有することをどのように確認すべきなのか及びどのように上記 a. 及び b. の要件を満たすべきかについて特段の定めを置いていない。GDPR のように標準的契約条項(Standard Contractual Clauses)や拘束的企業準則(Binding Corporate Rules)が上記 a. の要件を満たす方法となり得る可能性もあるが、この点は今後制定される下位規則の内容次第だと思われるので、今後の動向を注視する必要がある。

なお、インドネシアでは、PDP 法制定以前から、個人データを国外移転する際に一定の場合には通信情報省への報告が求められているが、当該義務は PDP 法制定後も有効である。

## 12. データブリーチに関する通知

PDP 法では、管理者は、「個人データ保護の失敗」が発生した場合、遅くとも 72 時間内にデータ主体及び監督当局に書面で通知する必要があるとされている。また、「個人データ保護の失敗」とは、機密性、完全性、可用性の観点から個人データを保護していないことであり、故意か否かを問わず、送信、保存又は処理されている個人データの破壊、損失、改変、漏洩、不正アクセスにつながるセキュリティ侵害を含むと定義されている。



このように「個人データ保護の失敗」が広く定義されているにもかかわらず、PDP 法には、GDPR と異なり、データ主体の権利自由に対するリスクが低い場合は通知義務が発生しないことを示す明文規定は存在しない。そのため、通知義務が発生する/しないデータブリーチの範囲をどのように画するのか不明確であり、下位規則での明確化が望まれる。

また、PDP 法には、「個人データ保護の失敗」が公共サービスに支障をきたす場合又は公共の利益に重大な影響を及ぼす場合、管理者は当該失敗について公表する必要があると定められている。

### 13. コーポレートアクションに関する通知

PDP 法では、合併、統合、買収、分割又は解散を行おうとする管理者は、事前及び事後の 2 回、データ主体に対して個人データの移転について通知しなければならないとされている。当該通知は、データ主体に対して個別に又は新聞による公表で行うことができる」とされている。

### 14. ペナルティ

PDP 法には、行政処分と刑事罰の 2 種類のペナルティが定められている。具体的には、適法性の根拠等のデータ保護に関する義務に違反した場合、警告、データ処理の一時停止、個人データの削除、制裁金(金額のレンジは未定)等の行政処分が課され得ることになる。さらに、以下の禁止事項が意図的に違反された場合、40~60 億ルピア(約 3500 万円~5000 万円)の罰金及び/又は 4~6 年の禁固刑の刑事罰の他に、犯罪行為による収益の没収等の追加刑が科され得ることになる。

- a. 自己又は他人の利益を図る目的で、データ主体に損失を与える不正な個人データの収集を行うことの禁止
- b. 他人の個人データを不正に開示することの禁止
- c. 他人の個人データを不正に利用することの禁止

また、刑事罰が科される行為が法人により行われた場合、経営者、管理者等にも刑を科することができる他、当該法人に対する罰金は上限が 10 倍となり、当該法人に下記の追加刑も科され得ることになる。

- a. 犯罪行為による収益の没収
- b. 会社の事業の全部又は一部の停止
- c. 特定の行為の永久的な禁止
- d. 会社の事業所の全部又は一部の閉鎖
- e. 違反された義務の履行
- f. 損害賠償
- g. ライセンスの取消し
- h. 会社の解散

### 15. 法令対応作業について

上記では、法令文言のみに基づいて PDP 法の規制内容を紹介したが、法令文言には抽象的な規定のみが定められており、適用の有無や実施すべき措置が不明確な義務も存在する。そのような規定は、今後制定される予定の下位規則によって一定の指針が示されることが予想される。

もっとも、下位規則がいつ頃までに制定されるかについて、現時点で具体的な見通しを立てることは困難である。インドネシアのような新興国では法令制定の遅延は日常茶飯事であり、重要な下位規則が制定されないまま猶予期間が経過して法令が全面施行され、その後に徐々に下位規則が制定されていくことも珍しくない(例えば、タイでは 2022 年に下位規則が全く制定されない状態で個人情報保護法が全面施行された)。

そのため、下位規則が全て制定されるのを待っている、いつまで経っても法令対応作業が開始できないことになり得る。データ保護法の法令対応作業には一定の時間を要するのが通常であるため、下位規則について今後の動向を注視しつつ、法令文言から可能な範囲で法令対応作業を開始することが望ましいと思われる。弊所は GDPR 対応に加えてアジア新興国の個人データ保護法対応についても豊富な経験を有するため、PDP 法の法令対応作業についてご不明点やお悩み等があればいつでもご連絡いただきたい。

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合ったトピックを解説したニュースレターを執筆し、随時発行しております。N&A ニュースレター購読をご希望の方は [N&A ニュースレター 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。

本ニュース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](#) 