

2018年2月

アセアン各国の個人情報保護法

2017年5月30日に、個人情報の保護を図りつつ、パーソナルデータの利活用を促進することによって新産業・新サービスの創出を後押しするとともに国民の安全・安心の向上を図ること等を目的とした¹、改正個人情報保護法が施行されました。

同改正により、第三者提供に関する規制が新たに追加されています。具体的には、トレーサビリティの確保（第三者提供に係る確認及び記録の作成義務）が義務付けられ、また、外国にある第三者への個人データの提供に関する規制も加わりました。

このため、ASEAN諸国に対して個人データを提供する事業を行う場合には、当該国がどのような内容・レベルの個人情報保護法制を採用しているかについて確認する必要があります。さらに、現地法人を有する事業者においては、日本の個人情報保護法のみならず当該国の個人情報保護法についても遵守するよう、ガバナンスをきかせることが求められています。

そこで、本ニューズレターでは、ASEAN10か国のうち、シンガポール、マレーシア、フィリピン、ベトナム及びインドネシアにおける個人情報保護法制を俯瞰します。

シンガポールの個人情報保護法制

1 シンガポールの個人情報保護法制の概要

シンガポールでは、2014年7月2日に“Personal Data Protection Act 2012”（個人データ保護法、以下「PDPA」といいます。）が全面施行されています。

¹ 個人情報保護法改正法案概要（<http://www.cas.go.jp/jp/houan/150310/siryoul.pdf>）

PDPAは、全10章からなっており、PDPAの監督機関にあたる“Personal Data Protection Commission”（個人データ保護委員会、以下「PDPC」といいます。）の設置、PDPAの保護対象となる“personal data”（個人データ）の保護の一般原則、個人データの収集、使用および開示、個人データの取扱い等、個人データ保護に関する規定と、我が国にはない、“Do Not Call Registry”という制度²について定めています。

PDPAには、個人データ保護に関する規則、命令および通達複数あるほか、PDPCによるPDPAの解釈について、PDPCが公表している各種ガイドラインがあり、シンガポールにおける個人情報保護法制を確認する際には、それらのガイドライン等にも目を通す必要があります。

2 日系企業への影響（適用対象）

PDPAの適用対象は、“organization”（団体等）とされていますが、これには、シンガポール法に基づき設立され、あるいは承認されたものかどうかを問わず、また、シンガポール居住者やシンガポール国内に営業所を設置しているかどうかを問わず、あらゆる個人、会社、組織ないし団体（法人であるかどうかを問わない。）が含まれるとされています。したがって、日系企業の子会社であるシンガポール法人は勿論のこと、日系企業の支店や駐在員事務所も幅広く適用対象となるため留意が必要です。

なお、我が国の個人情報保護法については、直近の改正で小規模事業者の適用除外規定が見直されましたが、PDPAにもそういった包括的な適用除外規定は設けられていませんので、シンガポールにおいて個人情報を取り扱う限り、適用対象となります。

3 「個人データ」とは

² PDPA第10章

【執筆者】アセアンプラクティスグループ
〈担当メンバー〉

- 弁護士 阿久津 匡美（総論担当）
- 弁護士 荒川 雄二郎（シンガポール担当）
- 弁護士 下西 正孝（マレーシア・フィリピン担当）
- 弁護士 生田 美弥子（ベトナム担当）
- 弁護士 坂元 靖昌（インドネシア担当）

本ニューズレターは法的助言を目的するものではなく、個別の案件については当該案件の個別の状況に応じ、弁護士の助言を求めて頂く必要があります。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、当事務所又は当事務所のクライアントの見解ではありません。本ニューズレターの発送中止のご希望、ご住所、ご連絡先の変更のお届け、又は本ニューズレターに関する一般的なお問合せは、下記までご連絡ください。

北浜法律事務所・外国法共同事業 ニュースレター係
(TEL: 06-6202-1088 E-mail: newsletter@kitahama.or.jp)

- 〔大阪〕 北浜法律事務所・外国法共同事業
〒541-0041 大阪市中央区北浜1-8-16 大阪証券取引所ビル
TEL 06-6202-1088 (代) / FAX 06-6202-1080-9550
- 〔東京〕 弁護士法人北浜法律事務所東京事務所
〒100-0005 東京都千代田区丸の内1-7-12 サビアタワー14F
TEL 03-5219-5151 (代) / FAX 03-5219-5155
- 〔福岡〕 弁護士法人北浜法律事務所福岡事務所
〒812-0018 福岡市博多区住吉1-2-25
キャナルシティ・ビジネスセンタービル4F
TEL 092-263-9990 / FAX 092-263-9991
<http://www.kitahama.or.jp/>

PDPA の保護対象となる “personal data” (個人データ) とは、真実であるかどうかを問わず、当該データにより特定されうる、あるいは、当該データとある団体が保有し、もしくはアクセス可能な情報により特定されうる個人についてのデータをいいます。ここにいう「個人」とは、自然人のみを指し、シンガポール国民やシンガポール居住者に限られず、外国人も含まれます。

このような個人データの定義は、我が国の個人情報保護法における個人情報の定義と重なるものと言えますが、我が国の個人情報保護法とは異なり、死者(死後 10 年超の者は除く。)も「個人」に含まれるとされている点に留意が必要です。

なお、ここにいう「データ」は、特にデータ化された情報や電子的な形態のものに限られるものではなく、個人に関するあらゆる情報、すなわち、個人の健康状態、学歴や雇用歴、消費パターンなどに関する情報一般を含むものとされています。

さらに、個人データのうち、当該データのみで個人を特定可能であり、それ自体が個人データとなるものは、PDPA に関する各種ガイドラインにおいて、“unique identifier” (識別符号)と呼ばれています。PDPC は、一般的に、氏名、NRIC (国民登録番号カード) 番号、FIN (外国人登録番号)、パスポート番号、携帯電話番号、顔の写真・ビデオ画像、声、指紋、虹彩画像、遺伝子情報などを識別符号として取り扱うとされています。

以上に対し、PDPA は、“business contact information” (仕事上のコンタクト情報)、具体的には、個人の名前、役名ないし肩書、仕事上の電話番号、住所、E メールアドレス、ファックス番号その他のこれらに類する個人についての情報で、個人的な目的のためだけに提供されたものではないものについては、後記のデータ保護規定の適用外としています。

4 個人データ保護に関する義務

PDPA は、第 3 章から第 6 章に、以下のような、個人データ保護に関して、PDPA の適用対象となる団体等が遵守すべき 9 つの主な義務を定めており、それらの規定は、まとめて “Data Protection Provisions” (データ保護規定)と呼ばれています。

なお、①の同意取得義務については、PDPA の別紙 2～別紙 4 に、個人データの取得、使用、開示のそれぞれの場面について、同意取得義務が免除される場合が定められており (PDPA 第 17 条)、④のデータ提供義務については同じく PDPA の別紙 5 に、是正義務については別紙 6 に、それぞれの義務が免除される場合が定められています (PDPA 第 21 条第 2 項、第 22 条第 7 項)。

① 同意取得義務 (PDPA 第 13 条～第 16 条)

- ② 目的遵守義務 (PDPA 第 18 条)
- ③ 告知義務 (PDPA 第 20 条)
- ④ データ提供・是正義務 (PDPA 第 21 条～第 22 条)
- ⑤ 正確性維持義務 (PDPA 第 23 条)
- ⑥ データ保護義務 (PDPA 第 24 条)
- ⑦ データ削除義務 (PDPA 第 25 条)
- ⑧ データ移転制限義務 (PDPA 第 26 条)
- ⑨ 内部規則等制定・公表義務 (PDPA 第 11 条～12 条)

5 シンガポール国外へのデータ移転

シンガポール国外への個人データの移転については、上記 4 の⑧のデータ移転制限義務により、移転されるデータについて、PDPA に基づく保護と同水準の保護が移転先でも与えられることが確認されない限り、シンガポール国外への個人データの提供は許されないとされています (PDPA 第 26 条第 1 項)。

6 PDPA 違反の場合の罰則等

PDPA に違反した場合の一般的な罰則としては、1 万シンガポールドル以下の “fine” (罰金) および/または 3 年以下の懲役とされています (PDPA 第 56 条)。

法人等による PDPA 違反が、取締役や役員らの同意や任務懈怠による場合には、それらの取締役や役員らも法人等と並んで個人責任を負うものとされているほか (PDPA 第 52 条)、従業員による違反行為は雇用主がそれを知っていたかどうかを問わず、雇用主の違反行為として扱われ、その責任を負うものとされています (PDPA 第 53 条)。

また、上記とは別に、個人データ保護委員会は、特にデータ保護規定の違反について、同委員会が適切と判断した場合、違反を犯した団体等に対し、個人データの収集、使用、開示の停止、収集済みの個人データの廃棄、一定期間内の個人データの提供や是正を指示するほか、100 万シンガポールドルを超えない範囲で、“financial penalty” (過料)を課すことができるとされています (PDPA 第 29 条)。個人データ保護委員会のウェブサイトで公表されている同委員会による処分事例は、本稿執筆時点で合計 36 件に上っています。

7 PDPA の改訂方針等

PDPC は、2017 年 7 月 27 日、同日開催の第 5 回個人データ保護セミナーにおいて、PDPA について、以下の二つの改訂方針を明らかにしています。

① 同意取得義務の例外

(ア) 個人データの収集、使用、開示に際して、同意の取得が現実的でなく、かつ、それらの収集、使用、開示が当該個人に不利益を与えな

いと考えられる場合は、目的を通知することで、同意を取得することなく、個人データの収集、使用、開示を認める。

- (イ) 一定の法的またはビジネス上の目的があり、当該目的のためには、同意の取得が却って適切ではなく、かつ、当該個人の被る不利益よりも公共の利益が明らかに大きい場合には、目的を通知することなく、同意を取得することなく、個人データの収集、使用、開示を認める。

② PDPC への通知義務

個人データの漏洩により、漏洩の対象となった個人に何らかのリスク、不利益または損害を生ずる場合には、当該個人と PDPC に対し、500 名以上の個人に関する個人データの漏洩など、大規模な個人データの漏洩があった場合には、PDPC に対し、それぞれ通知（漏洩の対象となった個人には可能な限り速やかに、PDPC には漏洩を認識してから 72 時間以内に）を行うものとする。

PDPC は、同日、グループ企業等、複数の団体等の間で、個人データを共有する場合、一定の要件を満たすことにより、PDPA の定める義務の一部を免除する取扱いに関するガイドライン（“Guide to Data Sharing”）を公表したほか、既存の公表済みのガイドラインの一部についても改訂を行っています。また、PDPC は、併せて、2018 年中の“Data Protection Trustmark”（認証制度の導入）や、APEC の“Cross-Border Privacy Rules”（システム等への参加方針）を表明しています。

このように、PDPC は、シェアリングエコノミーの拡大や IoT、機械学習、AI といったテクノロジーの発展に対応すべく、アジアのビジネスハブとしてのシンガポールにおける、より柔軟かつ信頼性の高い個人情報保護法制の確立を目指しているものと考えられます。

マレーシアの個人情報保護法制

1 本法の概要

マレーシアでは、2013 年 11 月 15 日から“Personal Data Protection Act 2010”（個人情報保護法、以下「本法」といいます。）が施行されています。本法の主な目的は、民間における商業的取引に関する個人情報の処理を規制することであり（本法 2 条（1）(b)）、連邦政府や州政府には適用がありません（本法 3 条(1)）。

また、本法違反の場合には、罰則（懲役及び罰金）の適用もあります。

2 日系企業への影響（適用対象）

本法は、マレーシア法人のみならず、マレーシア国外で設立された法人でも、個人情報を処理するためにマレーシアにおいて設備を使用する場合には適用されるとされており（本法 2 条（2）(b)）、マレーシア法人以外でも適用の可能性があります。

マレーシア国外において個人情報を処理する場合（但し、さらにマレーシア国内において個人情報を処理する意図が無い場合に限る）には、本法の適用は無いと考えられていますが（本法 3 条(2)）、後述のとおり、個人情報をマレーシア国外に送信することに対する制限がありますので、その点、留意が必要です。

3 「個人情報」とは

本法において、「個人情報」とは、商業的経済取引に関連する情報で、“data user”（情報使用者）が持つ当該情報から又は当該情報とその他の情報を併せて特定できる“data subject”（情報対象者）に直接又は間接に関連するものを意味します。身体・精神的な健康状態、政治的意見、宗教的信条等については、センシティブな個人情報として後述のとおりさらに厳しい取り扱いが求められます。（本法 4 条）。

4 遵守すべき原則

本法では、概要以下の 7 つの事項を遵守することが求められています（本法 5 条～12 条）。

- ①個人情報の処理につき、情報対象者の同意（センシティブ情報の場合には明確な同意）が必要。
- ②情報対象者に対する所定の事項を書面により通知することが必要。（なお、この通知は、マレー語及び英語で行われなければならない点注意が必要です。）
- ③情報対象者による個人情報へのアクセス・訂正を認めることが必要。
- ④個人情報収集時の目的以外で第三者に開示する場合には情報対象者の同意が必要。
- ⑤個人情報を収集した目的のため不要になった場合には、当該個人情報を破棄することが必要。
- ⑥個人情報の紛失や不正使用防止のための具体的な対策を採ることが必要。
- ⑦情報使用者は、収集した個人情報が正確で、完全に誤解を招かないものであり、又常に最新のものとなるよう合理的な措置を採る必要がある。

5 個人に認められている権利

本法に基づき、原則として、情報対象者個人に対して以下の権利が認められています。

- ①個人情報にアクセスする権利（本法 30 条）

- ② 個人情報を訂正する権利（本法 34 条）
- ③ 個人情報処理に関して同意を取り下げる権利（本法 38 条）
- ④ 損害等が発生する可能性がある場合に、個人情報の処理を妨げる権利（本法 42 条）
- ⑤ ダイレクトマーケティングのための個人情報利用を止めさせる権利（本法 43 条）

特に上記⑤については、個人情報主体から、かかる利用を止めるよう通知が来てもこれに従わなかった場合には、罰金が科せられる可能性があるため、注意が必要です。

6 Personal Data Protection Commissioner への登録

一定の場合（“Pawnbrokers Act 1972”に基づいてライセンスを受けている質屋、“Moneylenders Act 1951”に基づいてライセンスを受けている貸金業者などが該当するとされています。）には、Personal Data Protection Commissioner への登録が必要となります（本法 14 条）。

7 個人情報処理をマレーシア国外にて処理する場合の注意点

本法では、収集した個人情報をマレーシア国外に送信することが制限される場合があることに注意が必要です（本法 129 条）。かかる制限には一定の例外が定められており、対象者が同意している場合には、かかる例外に該当するとされているため、マレーシア国外において個人情報を処理することが想定される場合には、個人情報取得に際して、国外送信に関しても予め同意を取得しておくことが有益と言えます。

フィリピンの個人情報保護法制

1 本法の概要

フィリピンでは、2016 年 8 月 24 日に個人情報保護法の施行規則（以下、「本法」といいます。）が公布されました。

本法は、フィリピンにおける個人情報について定め、その取扱いについて定めるとともに、個人情報管理及び個人情報処理者に対して、個人情報保護のために、合理的かつ適切な、組織的、物理的及び技術的なセキュリティ対策を実施することなどを求めています。また、本法違反の場合には、罰則の適用もあります。

2 日系企業への影響（適用対象）

フィリピン国内で設立された法人の他、フィリピン国外で設立された法人であっても、フィリピンに事務所や支店を設置するなどして個人情報を取り扱う場合は、本法の適用対象となります。フィリピンにおいてビジネスを行い、顧客（個人）の情報を取得したり、従業員を

雇って従業員の個人情報を取得する場合には、幅広く適用の可能性がある点留意が必要です。

3 「個人情報」とは

① 個人の身元が明らか（若しくは確定しうるもの）となる情報、② 他の情報と組み合わせることにより個人を特定しうる情報が「個人情報」に該当します。個人情報の取得などをする場合には、個人情報の主体が同意していることなどが必要となります。フィリピン人やフィリピン居住者の個人情報に限定されるものではありません。また、本法では、特に取扱いに慎重を要する情報が「センシティブ個人情報」とされています。具体的には、① 個人の人種、民族、婚姻の有無、年齢、肌の色、宗教、政治的信条報、② 個人の健康状態、学歴、遺伝・性生活、前科前歴、③ 社会保障番号、納税申告、④ 行政命令・その他法令で特に定められた情報などを含みます。個人の年齢、学歴、健康状態など一般的に企業が取得する情報もセンシティブ個人情報の中に含まれますので注意が必要です。センシティブ個人情報の取得などをする場合には、個人情報の主体が同意する際に、原則として利用目的が特定されていることなどが必要となります。

4 個人情報が権限のない者に取得された場合

もし、管理する個人情報が権限のない者に取得された場合には、個人情報の主体が重大な損害を受ける現実的なおそれがあるときは 72 時間以内に NPC（National Privacy Commission）及び当該個人に書面で通知する必要があります。

5 セキュリティー対策

以下の通り、① 組織的、② 物理的、③ 技術的なセキュリティ対策を講じることが義務づけられています。

① 組織的なセキュリティ対策

- ・ 本法を遵守するための監督者を選任
- ・ 個人情報保護に関する社内規定の作成
- ・ 個人情報の処理に関する記録の実施
- ・ 個人情報にアクセスできる従業員等を選定し、これを監督
- ・ 個人情報の処理手続を向上及び見直し
- ・ 外部委託先において本法が遵守されているかの確認

② 物理的なセキュリティ対策

- ・ 電子媒体の適切な使用に関するガイドラインを定めるなど、情報の集積する場所をモニタリングし、アクセスを制限する社内規定を導入
- ・ 個人情報の処理をする者が適切に情報管理できるだけの作業場所を確保
- ・ 個人情報を処理する者の義務、責任等の明確化
- ・ 個人情報の適切な保護のために、電子媒体の破棄や再利用などに関する社内規定の導入
- ・ 個人情報を含むファイルや機器が自然災害や外部からのアクセスにより破壊されることを防ぐための社内規定の導入

③ 技術的なセキュリティー対策

- ・コンピューターネットワークを保護するための安全措置
- ・個人情報を処理するシステムやサービスの機密性や利用可能性の維持・確認
- ・セキュリティー違反がないか定期的なモニタリングの実施
- ・物理的・技術的な問題が生じたときに速やかに修復できる体制の整備
- ・セキュリティー対策が効果的であるかについて定期的な検証
- ・個人情報やアクセスを制限する技術的なセキュリティー対策に関する暗号化

6 NPC への登録

従業員数や、処理するセンシティブ情報の対象人数に応じて、一定の場合、個人情報を処理するシステムについて、NPC に登録する必要がある点留意が必要です。

7 個人情報処理を外部業者に委託する場合の注意点

本法では、個人情報の処理を外部業者に委託する場合に契約で定めておかなければいけない事項が規定されています。

契約において規定することが求められている事項（主なもの）

- ・個人情報管理者の指示に基づいて処理を行うこと
- ・秘密保持義務
- ・適切なセキュリティー対策を講じ、本法を遵守
- ・個人情報管理者の事前の指示なく、別の処理者を関与させないこと
- ・データ主体からの求めなどに応じる義務を履行することができるように個人情報管理者を支援すること
- ・個人情報管理者が、本法等の遵守するために援助を行うこと
- ・業務が終了した場合には、個人情報管理者の求めに応じて、個人情報を返却又は消去すること
- ・本法の義務の遵守を証明するために必要な、すべての情報を個人情報管理者に提供すること
- ・個人情報管理者の指示が本法等に違反する場合には、直ちに通知すること

8 本法違反の場合の罰則

本法違反の行為について、行為に応じて最大7年の懲役刑及び400万ペソの罰金（複数の行為に該当する場合には加重の可能性があります。）が科せられます。また法人の役員に対して罰則が科せられることがあること、及び外国人に対しては国外退去処分が科せられる点も理解しておくべきです。なお、本法違反行為については、民事上の責任を負う場合があることに注意が必要です。

ベトナムの個人情報保護法制

1 個人情報保護法の規定がないこと

ベトナムでは、個人情報保護を主たる目的とする法令は定められていません。そのため銀行、消費者保護、IT業界、テレコミュニケーション等、事業単位での規制がなされているにとどまります。もっとも、サイバースペースにおける情報保護を目的とする2015年11月19日付“Law on Cyber-Information Security (LCIS)”（サイバー情報セキュリティ法）ができ、その中で個人情報の保護についても規定していますので、その概要をご紹介します。

ベトナムでは2009年のIT法、2013年のインターネットの使用管理を定める72号規則、e-コマースを規律する52号規則の中でも、個人情報について規定されていますが、LCISの定める個人情報の定義の方が広いと考えられています。

LCISは企業にも個人に対しても適用されます。また、公的私的を問わず情報ネットワークに対して適用されます。個人情報の収集、使用、改訂、削除を規定し、情報の管理者が個人情報を収集した当初の目的が失われた場合や、当初予定の期間を満了した場合には、個人情報は削除されなければならないといった定めも置かれています。LCISの下では、本人の承諾を得ずに個人情報を収集、使用、拡散、譲渡したり、情報システムの脆弱性を利用して個人情報を集めたり利用する行為は罰則の対象になるとされています。もっとも、LCISで個人情報が保護されるのは、個人情報の処理が「商業目的」による場合に限られるとされているところ、この「商業目的」とは何か、LCIS上には定義されていません。

また、LCISでは、個人や組織の情報処理に対し法令順守しているかどうかについて、自主的に、または個人からの告発がある場合に、政府当局は、LCISに基づき調査する権限を有すると定めています。

なお、個人の権利として肖像権や、一定の個人情報の秘密性を保障する権利などは、別途民法で定められています。

2 日系企業への影響（適用対象）

LCISは、サイバーセキュリティ目的のため、ベトナム政府が、企業や個人に対し、協力を要請することができますと定めています。しかし、企業や個人が、当局からどのような協力を要請されるのかは定められていません。なお、当局から要請を受けたのに、その指示にも拘わらず第三者の電子情報をモニターすることを怠ったり、テロリストの行為その他の刑事上の違反に関係したユーザーの個人情報を開示することを怠ったときは、当局から50万ドン（約100万円）の罰金が科せられるとされています。

その他の罰金規定として、個人のプライバシーに関する権利の侵害に関し、LCIS 以外の特別法によって罰金が科されることもあります。例えば、顧客の個人データを e-コマース取引で承認なく開示すると、60 から 80 百万ドルの罰金、事前に同意を得ることなく、個人からその個人情報を収集、処理、使用するにあたり、適切な保護措置を用意しなかった場合には、10 から 20 百万ドルの罰金、受領者の事前の同意なくダイレクトメールや、電子メールで広告を送付すると 30 百万ドルの罰金が科されることになっています。

3 「個人情報」とは

LCIS 以前、例えば 72 号規則では、名前、年齢、住所、ID カード番号、電話番号、電子メールアドレス、その他法に定める情報を含む個人に関連する情報が「個人情報」とされていました。

LCIS では、「個人情報」とは、ある人を特定する情報を指すと定義し、個人情報の所有者はその情報によって特定される人と定めています。このような定義は、それまでの IT 法等の規則の定義に比べて抽象的であり、より広い保護が予定されていると考えられています。

インドネシアの個人情報保護法制

1 本法の概要

インドネシアでは、現在、労務管理、ヘルスケア、金融、電子取引等、事業単位で個人情報に関する規制がなされています。特に電子商取引に関しては、“Electric Information Law”（以下「電子情報法」といいます。）が定められており、同法の施行規則である「電子商取引における個人情報保護に関する規則（2016 年商務省規則第 20 号）」（以下「個人情報保護規則」といいます。）が 2016 年に発効され、電子情報に関して個人情報保護に関する規制が強化されました。そこで、本項では、電子情報法並びに個人情報保護規則（以下、両者合わせて「同法令」といいます。）についてその概要をご紹介します。なお、本法令の成立は 2016 年 12 月ですが、2 年間の猶予期間が設けられています。³

2 適用主体

同法令において規制される主体は、“Electric System Provider”（電子システム提供者、以下「ESP」といいます。）と定義されており、電子システムを用いるものは幅広く本法令で規制しています。ESP は「あらゆる人、国家機関、事業法人または共同体で、独立してまたは共

同して、電子システムユーザー及び／又は、ほかの法主体の利益のために、電子システムを提供し、監督し、運営するもの」と定義されており、かなり広い範囲で ESP に該当する可能性があるという点に留意が必要です。また ESP となるには、証明を受ける必要があるとされていますが、証明の詳細については下位法令で具体化するとされており、未だに明確になっておりません。“

3 監督官庁

同法令による規制は、“The Minister of Communication and Informatics”（通信情報省、以下「MOCI」といいます。）によって所管されます。MOCI は担当官庁として、ESP の情報管理体制をチェックするだけでなく、ESP と個人情報提供者間で紛争が生じた場合に調停したり、個人情報をインドネシア国外に移す場合に調整したりする役割が期待されています。

4 情報保管場所

上述のとおり、ESP は、私法人のみならず国家機関や国営会社も含まれ、公共サービスを所管する ESP（例、インドネシア国営電力会社や、大手携帯電話会社である PT テレコムニカシ等）の場合は、データセンターをインドネシア国内に設置し、自然災害等の場合に復旧できるように復旧センターを設置することがそれぞれ義務付けられています。

5 保護対象

同法令で保護される「個人情報」とは「個人を直接または間接に特定することができる正確かつ実際の情報」を指すものとされています。そしてその情報の取得、収集、保管、加工、分析、提供、公表等、個人情報の各段階の行為がそれぞれ規制されています。保管や加工等の行動は個人情報取得時に個人情報提供者に対して明示された目的に従ってのみ許されることとなります。

6 個人情報取得時に課せられる同意取得義務

ESP は、個人情報取得時点で、①個人情報収集の目的、②将来個人情報を加工するに当たり関連してくるであろう目的、③個人情報の管理に関する連絡先を通知する必要があります。

さらに個人情報を加工するにあたっては明示的に同意を書面で取得する必要があります（電子媒体でも構いません）。インドネシア固有のルールであり、同意を書面で取得するにあたってはインドネシア語で行われることとされていますが、二言語併記（たとえば英語及びインドネシア語）で行うことは禁止されていません。

なお、個人情報を国外に移転する場合には、MOCI に対して当該情報移転を「調整」する必要があるとされていますが、具体的にどのような状況で、どのような手続をしなければならないのか等、不明な点が多く今後の具体化が待たれます。

³ なお、インドネシア国会において、一般的な個人情報保護法が審議されておりますが、2018 年 1 月現在ではまだ施行されておられません。

7 その他保護主体に課せられる義務

ESP は、上記のとおり種々の義務が課せられていますが、その他にも①体制及び②情報管理に関して種々の義務が課せられています。すでにご説明したものと合わせて主要な部分は、以下のとおりです。

① 体制に関する義務

- ・ ESP として証明を受けること。
- ・ ESP としてシステムを運用する能力およびシステムの互換性を確保し、合法的なソフトを用いること。
- ・ 個人情報保護に関する内部規則を定めること。
- ・ 個人情報管理に関して、個人情報提供者が容易に連絡することができる担当者を選任すること。
- ・ 公共サービスを提供する ESP はデータセンターや復旧センターをインドネシア国内に設けること。

② 情報提供者との間の義務

(情報取得時点の義務)

- ・ 情報取得に際して目的を公表又は開示すること。
- ・ 個人情報提供に際しての書面または電磁的書面で同意を取得すること（インドネシア語での同意取得が必要）。
- ・ ESP の個人情報管理の担当者の連絡先を個人情報提供者に通知すること。

(管理・第三者提供時の義務)

- ・ 個人情報の管理・加工等は、当該目的の範囲内において行うこと。
- ・ 個人情報の正確性を確保し、個人情報提供者に情報へのアクセスを認め、修正もしくは更新できるようにすること。
- ・ 個人情報を暗号化した形式で保管し、個人情報提供者が、当該 ESP のシステム利用を終了した後も、5 年間は当該情報を保管すること。
- ・ ESP が取得した個人情報を第三者に提供する際には、個人情報提供者に対して、情報提供を許諾するか否かにつき同意する機会を与えること。
- ・ ESP が個人情報をインドネシア国外に移転する場合は、MOCI と調整すること。
- ・ 個人情報の不正流出が発覚した場合は、個人情報提供者に対して発覚してから 14 日以内に通知すること。

8 義務違反の場合の制裁

ESP には上記の通り各種義務が定められていますが、これに違反した場合、まず行政上の制裁として①口頭または文書による警告、②事業活動の一時的中止、③当該違反の公表などの制裁を課せられます。

9 日系企業への影響

かなり広範囲に ESP の概念を定義しているため、日系企業も同法の適用をまぬがれることができません。特に ESP としての証明取得、個人情報取得時点での同意取得、目的の公表等の対応や社内体制の構築など、対応しなければならない項目が多いので、今後の細則等について、注視しておく必要があるかと思われます。

以上