NISHIMURA & ASAHI

西村あさひ法律事務所

ガイドライン及び Q&A の内容を踏まえた 2020 年改正個人情報保護法への対応

個人情報保護・データ保護規制ニューズレター　2021 年 12 月 27 日号

執筆者:
E-mail 岩瀬 ひとみ
E-mail 菊地 浩之
E-mail 河合 優子
E-mail 村田 知信
E-mail 五十嵐 チカ
E-mail 松本 絢子
E-mail 菅 悠人

目次

Ⅰ　ガイドライン及び Q&A の内容を踏まえた 2020 年改正個人情報保護法への対応

1.　はじめに

2021 年も残りわずかとなり、2020 年改正個人情報保護法(以下「改正法」)の全面施行日である 2022 年 4 月 1 日が近付いている。改正法の全面施行に備えた対応は急務であるが、8 月に公表された改正法に伴う個人情報保護法のガイドライン(以下「改正ガイドライン」)及び 9 月に公表されたガイドライン等に関する Q&A(以下「改正 Q&A」)を踏まえた対応について、改正ガイドライン等で紙幅を割いて説明のなされている個人データ漏えいの際の報告及び通知、国外データ移転への同意を得る際に提供すべき情報並びに保有個人データの安全管理のために講じた措置の公表について検討する[1]。

2.　個人データの漏えい等の際の報告及び通知

(1)　報告期限

改正法により、一定の個人データの漏えい、滅失、毀損等の事態について個人情報保護委員会への報告が義務化され(法 26 条)、改正された個人情報保護法施行規則(以下「改正規則」)により、速報及び確報という 2 種類の報告が定められているところ(規則 6 条の 3 第 1 項及び第 2 項)、速報は、個人データ漏えい等の事態を知った後、「速やかに」報告するものとされており、具体的な期限は法令上は定められていない。

この点、改正ガイドライン(通則編)において、個人情報保護委員会の考え方が示され、「『速やか』の日数の目安については、個別の事案によるものの、個人情報取扱事業者が当該事態を知った時点から概ね 3～5 日以内である。」とされている(3-5-3-3)。また、「知った」時点については、「個別の事案ごとに判断されるが、個人情報取扱事業者が法人である場合には、いずれかの部署が当該事態を知った時点を基準とする。」との個人情報保護委員会の考え方が示されている(3-5-3-3)。さらに、改正 Q&A において、「部署が当該事態を知った」という意義について、「個別の事案ごとに判断されますが、部署内のある従業者が報告対象事態

[1] 2021 年改正個人情報保護法も改正法と同日に施行予定であり、これまで別個であった行政機関や独立行政法人を対象とする個人情報の保護に関する法律との一本化がなされている 2021 年改正個人情報保護法により現行の個人情報保護法とは条文番号が大幅に変更となる。本稿では、2021 年改正個人情報保護法による変更後の条文番号を記載している。

を知った時点で『部署が知った』と考えられます。」との考え方が示されている(A6-21)。

上記のとおり、部署に関して、例えば、個人データの管理責任を負う部署といった限定はなされておらず、従業員についても部署内の一定の地位にある者などの限定もない。そのため、極端に言ってしまえば、データ漏えい事故を起こした会社の個人データの保護に関する責務とは関係のない部署に所属する従業員の 1 名が、当該事故を認識した時点で、「個人情報取扱事業者が当該事態を知った時点」となり、そこから概ね 3～5 日以内で個人情報保護委員会に対して速報を行わなければならないということも十分に考えられる。「速報時点での報告内容については、報告をしようとする時点において把握している内容を報告すれば足りる。」とはされているものの(改正ガイドライン(通則編)3-5-3-3)、速報を行う際に最低限の事実確認などは行うものと思われるので、従業員がデータ漏えい等の事故を把握した時点で速やかに情報を吸い上げ、調査等を迅速に行い得る社内体制の整備及び当該社内体制の従業員への周知徹底が必要となろう。

なお、確報に関しては、報告対象事態を知った日から 30 日又は 60 日以内に報告しなければならないとされているが(改正規則 6 条の 3 第 2 項)、確報を行う時点において、「合理的努力を尽くした上で、一部の事項が判明しておらず、全ての事項を報告することができない場合には、その時点で把握している内容を報告し、判明次第、報告を追完するものとする。」とされた(改正ガイドライン(通則編)3-5-3-4)。これは以前パブリックコメントの回答の際に示されていたものが、ガイドラインに規定されたものとなる。また、確報の報告期限の算定に土日・祝日も含めるとされ、30 日目又は 60 日目が土日、祝日又は年末年始閉庁日(12 月 29 日～1 月 3 日)の場合は、その翌日を報告期限とするとされている(改正ガイドライン(通則編)3-5-3-4)。

(2) 報告及び通知義務から除外される高度な暗号化等の措置の具体例

上記のとおり、改正法において一定の個人データの漏えい等の事態につき、個人情報保護委員会への報告が義務付けられたが、高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じた個人データに関する漏えい等の事態は、報告の対象から除外されている(改正規則 6 条の 2 第 1 号)。

改正ガイドライン(通則編)においては、「漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合等、『高度な暗号化その他の個人の権利利益を保護するために必要な措置』が講じられている場合については、報告を要しない。」とされていて(3-5-3-1)、さらに、改正 Q&A においては、上記の「漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合」に該当するためには、(i)「当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等が発生し、又は発生したおそれがある個人データについて、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられる」とともに、(ii)「そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解され」るとしており、(i)の「第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストや ISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられ」るとしている(A6-16)。加えて、(ii)の「暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解され」るとしている(A6-16)。したがって、これらの要件を満たす個人データが漏えい等した場合には、個人情報保護委員会への報告を要しないが、後々、報告義務違反に問われないためにも、これらの要件を満たしていることを立証できるようにする必要があると思われる。

3. 国外データ移転への同意を得る際に提供すべき情報

改正法を受けた改正規則は、国外データ移転への同意を得る際に本人に提供すべき情報として以下を定めている(改正規則 11 条の 3 第 2 項)。

① 当該外国の名称
② 適切かつ合理的な方法により得られた当該外国における個人情報の保護に関する制度に関する情報
③ 当該第三者が講ずる個人情報の保護のための措置に関する情報

ただし、移転先の外国が決まっていない場合には、上記①及び②に代えて、以下の事項について本人に情報を提供しなければ

ならない(改正規則 11 条の 3 第 3 項)。
④　移転先の外国が特定できない旨及びその理由
⑤　移転先の外国の名称に代わる本人に参考となるべき情報がある場合には、当該情報
また、前記③に定める情報を提供できない場合には、提供できない旨及びその理由について情報を提供しなければならないとされている(改正規則 11 条の 3 第 4 項)。

上記のうち、②については、改正ガイドライン(外国提供編)において、「『当該外国における個人情報の保護に関する制度に関する情報』は、一般的な注意力をもって適切かつ合理的な方法により確認したものでなければならない」とされていて、その具体例として、提供先の外国にある第三者に対して照会する方法、日本又は外国の行政機関等が公表している情報を確認する方法が挙げられている(5-2(2)①)。
また、上記②のうち、「当該外国における個人情報保護に関する制度に関する情報」は、提供先の第三者が所在する外国における個人情報の保護に関する制度と個人情報保護法との間の本質的な差異を本人が合理的に認識できる情報でなければならず、具体的には以下の(ア)から(エ)までの観点を踏まえる必要があるとされている(改正ガイドライン(外国提供編)5-2(2)②)。
(ア)　当該外国における個人情報の保護に関する制度の有無
(イ)　当該外国の個人情報の保護に関する制度についての指標となり得る情報の存在
その具体例としては、当該外国が GDPR の十分性認定を受けていることや APEC の CBPR システムの加盟国であることが挙げられていて、(イ)の情報を提供した場合には下記(ウ)に関する情報の提供は求められない。
(ウ)　OECD プライバシーガイドライン 8 原則に対応する事業者の義務又は本人の権利の不存在
OECD プライバシーガイドライン 8 原則は、以下のものである
(i)　収集制限の原則(Collection Limitation Principle)
(ii)　データ内容の原則(Data Quality Principle)
(iii)　目的明確化の原則(Purpose Specification Principle)
(iv)　利用制限の原則(Use Limitation Principle)
(v)　安全保護措置の原則(Security Safeguards Principle)
(vi)　公開の原則(Openness Principle)
(vii)　個人参加の原則(Individual Participation Principle)
(viii)　責任の原則(Accountability Principle)
(エ)　その他本人の権利利益に重大な影響を及ぼす可能性のある制度の存在
その具体例としては、事業者に対し政府の情報収集活動への広範な協力義務を課すことにより、事業者が保有する個人情報について政府による広範な情報収集が可能となる制度や事業者が本人からの消去等の請求に対応できないおそれがある個人情報の国内保存義務に係る制度が挙げられている。

次に、改正ガイドライン(外国提供編)において、上記③の「当該第三者が講ずる個人情報の保護のための措置に関する情報」は、個人データ移転先が講ずる個人情報の保護のための措置と個人情報保護法により個人データの取扱について個人情報取扱事業者に求められる措置との間の本質的な差異を本人が合理的に認識できる情報でなければならないとされている(5-2(3))。具体例として、個人データ移転先が上記の OECD プライバシーガイドライン 8 原則に対応する措置を講じていない場合には、当該講じていない措置の内容について、本人が合理的に認識できる情報が提供されなければならないとされている(同上)。

他方で、先述したとおり、同意取得時に移転先の外国が特定できない場合には、上記の④(及び⑤)に関する情報を提供すれば足りるところ、⑤の「提供先の第三者が所在する外国の名称に代わる本人に参考となるべき情報」の例として、移転先の外国の範囲が具体的に定まっている場合における当該範囲に関する情報が挙げられている(改正ガイドライン(外国提供編)5-3-1(2))。
また、上記③の提供先が講ずる個人情報の保護のための措置に関する情報が提供できない場合の具体例として、改正ガイドライン(外国提供編)においては、製薬会社の治験時にどの国で医薬品等の承認申請を行うかが未確定である場合、再保険に関し、顧客からの同意取得の際にどの再保険会社に再保険を依頼するかが未確定である場合が挙げられている(5-3-2)。

4.　保有個人データの安全管理のために講じた措置の公表

改正法に伴う政令の改正により、保有個人データの安全管理のために講じた措置が法定公表事項に追加された(政令 8 条 1

号)。そもそも、安全管理措置は、「事業の規模及び性質、保有個人データの取扱状況(取り扱う保有個人データの性質及び量を含む。)、保有個人データを記録した媒体等に起因するリスクに応じて、必要かつ適切な内容としなければ」ならず、「当該措置の内容は個人情報取扱業者によって異なり、」公表する措置の内容も個人情報取扱事業者によって異なるとされており、具体的な基準は示されていないが、「『個人情報の保護に関する法律についてのガイドライン(通則編)』に沿って安全管理措置を実施しているといった内容の掲載や回答のみでは適切ではない」とされている(改正ガイドライン(通則編)3-8-1(1)④)。公表事項の具体例として、物理的安全管理措置につき、「個人データを取り扱う区域において、従業者の入退室管理及び持ち込む機器等の制限を行うとともに、権限を有しない者による個人データの閲覧を防止する措置を実施」や技術的安全管理措置につき、「アクセス制御を実施して、担当者及び取り扱う個人情報データベース等の範囲を限定」などがガイドライン上挙げられていることから、ある程度個々の措置についての記載が必要になると思われる。

他方で、本人の知り得る状態に置くことにより安全管理に支障を及ぼすおそれがあるものについては公表を要しないとされているが、その具体例として、ガイドライン上、以下の 4 つの事例が挙げられており(改正ガイドライン(通則編)3-8-1(1)④)、参考になるものと思われる。

事例 1)個人データが記録された機器等の廃棄方法、盗難防止のための管理方法
事例 2)個人データ管理区域の入退室管理方法
事例 3)アクセス制御の範囲、アクセス者の認証手法等
事例 4)不正アクセス防止措置の内容等

Ⅱ　個人情報保護・データ保護規制　各国法アップデート

1.　中国

- 2021 年 11 月 14 日、「インタネットデータ安全管理条例(意見募集稿)」が公表され、2021 年 12 月 13 日まで意見募集が行われた。
- 2021 年 11 月 12 日、「インスタントメッセージサービスプラットフォーム個人情報認定指針(意見募集稿)」が公表され、2021 年 12 月 12 日まで意見募集が行われた。

2.　米国

- 2021 年 11 月 8 日、米国ニューヨーク州の Civil Rights Law の改正法が、州知事による署名手続を経て成立した。同法では、規模の大小を問わず、ニューヨーク州に事業所を有する民間の雇用主は、従業員による電話、メール、インターネット利用等について電子的なモニタリングを行う場合、事前に従業員に通知をすること、また、同法施行後に雇用される従業員からは文書又は電子的方法により当該通知の確認を得ること等が義務付けられる。同法は、2022 年 5 月 7 日に施行される。

3.　ベトナム

- ベトナムでは、2021 年 2 月に、GDPR のコンセプトを取り入れつつ厳格な越境移転規制やセンシティブデータ処理に関する規制を導入する個人情報保護に関する政令案の草案が公表されていた。当該草案には 2021 年 12 月 1 日から施行される旨規定されていたが、当該施行予定日が経過した本稿作成時点においても、当該政令は未だ施行されていない。当局から施行延期の公式なアナウンスはされていないが、事実上延期されたのだと思われる。

4.　インド

- インドでは、2019 年 12 月 11 日に国会に個人情報保護法案(the Personal Data Protection Bill)が提出されていたが、2021 年 12 月 16 日に国会合同委員会が本法案に関する勧告報告書を提出した。従来個人情報保護法案は個人データのみを規律の対象としていたが、勧告報告書では法案を個人データと非個人データの両方を規制するものとすることが提案され、データ移転(特にセンシティブ個人データの海外への移転)の制限を強める等、大幅な修正が加えられている。また、ソーシャルメディアのプラットフォーマーの義務、児童や死者等のデータ主体ごとのデータの扱いに関する規律等、従来の法案

よりも多様な内容を含むものとすることが提案され、法案名も Data Protection Bill, 2021 に修正されている。現段階では、Data Protection Bill, 2021 は国会の審議対象となる法案としては提出されておらず、インド電子情報技術省によりさらに修正される可能性がある。

5. スリランカ

・ スリランカでは、2019 年 9 月、GDPR のコンセプトを取り入れた 2019 年個人データ保護法案がデジタルインフラ・情報技術省と法務起草部により策定され、公表されていた。当該法案はその後修正され、今般閣議決定が行われて国会に提出された(2021 年 11 月 25 日に官報に掲載された)。今後当該法案が国会で審議される予定である。

6. ブルネイ

・ ブルネイでは、2021 年 12 月 3 日、情報通信技術産業庁により同年 5 月 20 日に募集が開始された個人情報保護法(Personal Data Protection Order)のパブリックコメントに対する回答が公表された。同回答において、同庁は、同法を 2022 年半ばまでに施行すること、及び企業が同法に準拠するまでに 2 年間の猶予期間を設ける予定であることを明らかにした。同庁は、今後、企業による同法の遵守を支援するために、アドバイザリーガイドライン等の参考資料を発行する意向を示している。

7. アラブ首長国連邦（UAE）

・ アラブ首長国連邦(UAE)では、各首長国のフリーゾーンにおけるデータ保護法の見直しが相次いでいたところ、2021 年 9 月 20 日、連邦レベルでの個人情報保護法(Federal Decree Law No.45/2021 Relating to the Protection of Personal Data and Privacy)が新たに制定された。新法は 2022 年 1 月 2 日に施行され、今後新法の施行規則が公表される予定であるが、新法に基づく義務遵守に関しては、施行規則の公表から少なくとも 6 ヶ月の猶予期間が付与される見通しである。

・ 新法による規制内容は、概ね EU 一般データ保護規則(以下「GDPR」)と平仄を合わせているが、例えば以下のような相違点がある。

(1) 個人データ取扱に必要な同意取得義務の例外として、「データ管理者の正当な利益(legitimate interest)のために取扱が必要な場合」が挙げられていない。

(2) データ侵害の監督機関への通知期限につき、(GDPR の 72 時間より長い)10 日以内に行えば足りるとされている一方、影響評価を含めてより詳細な検討を重ねた上で通知を行う必要がある。

(3) (GDPR と同様、データ管理者は、データ主体からの要請に応じてデータ処理に関する一定の情報を提供する義務を負うものの、)当該情報提供が個人データの取得と同時に行われることまでは明示的には求められていない。

(4) データの取扱についてデータ処理者が複数いるが、データ管理者とデータ処理者間の契約がない場合、複数のデータ処理者は同法上の義務及び責任を相互に連帯して負う旨が明示されている。

(5) GDPR に比べてより詳細なデータ処理の過程を記録すべき義務が明示されている。

・ 新法は、連邦政府には適用されず、アブダビ首長国内の Abu Dhabi Global Market 及びドバイ首長国内の Dubai International Financial Centre といったフリーゾーン内で設立された団体には適用されない。また、連邦政府に関するデータ、独自のデータ保護規制に服する健康データ及びバンキング・信用情報データ等の特定のカテゴリーのデータは、新法の適用除外とされている。

8. オーストラリア

・ 2021 年 11 月 12 日、連邦政府は、Consumer Data Right(CDR)に関する規則(Competition and Consumer (Consumer Data

Right) Rules 2020)を改正し、2022 年 11 月より、CDR がエネルギー事業分野にも適用されることとなる。今後はエネルギー分野に続く事業分野として、電気通信分野への適用拡大が検討されている。本規則については、当事務所個人情報・データ保護ニューズレター2021 年 11 月 26 日号も参照されたい。

9. ニュージーランド

- 2021 年 11 月 10 日、プライバシーコミッショナーオフィス（OPC）は、賃貸住宅事業分野を対象にする新しい監督プログラムを公表した。この監督プログラムでは、OPC は不動産業者が Privacy Act 2020 を遵守しているかについて、年次監査等によって定期的な監督を行うとともに、法令違反者に対しては、勧告や指導、違反者の名前の公表等の処分が行われ、勧告に従わなかった不動産業者に対しては最大 10,000 NZ ドルの罰金が科されることとされている。また、新しい監督プログラムの公表にあわせて、OPC は、不動産業者向けのガイドライン等の資料を公表した。ガイドラインは不動産業者が個人情報を取り扱う際に遵守すべき諸原則を明らかにしており、借主との間で物件の賃貸借契約を締結するまでの各段階(内見、審査、契約締結など)において収集することができる個人情報の類型を例示し、収集する個人情報は必要最低限にとどめるべきであることなどを定めている。
- 2021 年 10 月 7 日、OPC は、生体認証情報の Privacy Act 2020 上の取扱に関する見解を公表した。この見解では、生体認証情報が Privacy Act 2020 の適用を受ける個人情報に該当することを明らかにするとともに、生体認証情報は特にセンシティブであるため、生体認証情報に関わる事業を実施する場合には、より慎重なプライバシー影響評価(PIA)を実施するべきであるとしている。

10. ルワンダ

- 2021 年 10 月 13 日、ルワンダ初のデータ保護法である「個人情報及びプライバシーの保護に関する法律」(Law No.058/2021 Relating to the Protection of Personal Data and Privacy)が制定され、同月 15 日に施行された。同法は、ルワンダ国内に所在する管理者及び取扱者に適用される他、ルワンダ国外に所在する管理者及び取扱者に対しても、ルワンダ国内に所在する個人情報を取り扱う限り適用される。

西村あさひ法律事務所　広報室　E-mail