

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✉ [井之上 旦](#)

E-mail✉ [五十嵐 チカ](#)

E-mail✉ [松本 絢子](#)

E-mail✉ [菅 悠人](#)

E-mail✉ [斎藤 公紀](#)

目次

- I 南アフリカにおけるデータ関連法制の最新動向／五十嵐 チカ、斎藤 公紀、井之上 旦
- II 個人情報保護・データ保護規制 各国法アップデート／岩瀬 ひとみ、松本 絢子、河合 優子、五十嵐 チカ、菊地 浩之、菅 悠人、村田 知信

I 南アフリカにおけるデータ関連法制の最新動向

1. はじめに

南アフリカでは、本年(2021年)、データ関連の法制について目覚ましい進展がみられたため、本稿では、そのハイライトとして下記3点を紹介する。

- ① 南アフリカの[個人情報保護法\(Protection of Personal Information Act\)](#)は、2013年の制定以来、段階的に施行されてきたが、2021年7月1日以降、同法違反の場合におけるエンフォースメントを含めて、主要な条項が全面的に適用されることになった。これに伴い、同法の規定内容を具体的に説明するガイダンスノートが複数発表されている。
- ② また、2021年4月23日には、司法憲法開発省(Department of Justice and Constitutional Development)が、2000年に制定された[情報アクセス促進法\(Promotion of Access to Information Act\)](#)に基づく[規則案](#)を発表した。
- ③ さらに、同年5月26日には、ラマポーザ南ア大統領の署名により、[サイバー犯罪法\(Cybercrimes Act\)](#)が成立した(施行日は未定)。

こうした動向を受け、南アフリカで個人情報を処理する事業者は、これら3種の法令の適用の有無を確認の上、それらを遵守するよう実務運用を進める必要がある。

2. 個人情報保護法

(1) 規制の概要

南アフリカにおいて、個人情報を保護する主な法令は、個人情報保護法であり、同法は、南アフリカで個人情報を処理している事業者1に適用される。適用対象となる事業者は、管理者(Data Controllers)と呼ばれ、管理者には、同法上、①情報責任者(Information Officer)/情報副責任者(Deputy/Vice Information Officer)に関する義務、②個人情報の収集における義務、③個人情報の処理における義務が課される。また、同法では、データブリーチ時において管理者が講じるべき対応なども規定されている。

¹ また、当該事業者が自ら個人情報を処理しなくとも、南アフリカで当該事業者のために個人情報を処理する者を選任する場合には、当該事業者に対しても個人情報保護法が適用される。

なお、同法に関する細則として、南アフリカの情報規制当局(Information Regulator)が² 2018 年に[個人情報保護規則\(Regulations Relating to the Protection of Personal Information\)](#)を制定・公表している。

(2) 管理者の義務

ア 情報責任者等に関する義務

個人情報保護法上、事業者の代表者は、自動的に同法上の情報責任者を担うものとされているが²、代表者以外の適切なレベルの役職員を情報副責任者として選任することもできる³。そして、情報責任者及び情報副責任者が担うべき具体的な義務・職務の内容は、(a)個人情報を適法に処理するためのコンプライアンス・フレームワークの策定・実施・チェック、(b)個人情報影響評価(Personal Information Impact Assessment)の実施、(c)データ主体による各種要求への対応、(d)個人情報保護に関する情報規制当局との連携などである⁴。

また、南アフリカで個人情報を収集・処理している事業者は、情報責任者及び情報副責任者を情報規制当局に登録する義務が課されている⁵。

イ 個人情報の収集における義務

管理者は、個人情報を収集する際、原則として、それに先立ち又は収集後可能な限り速やかに、次の事項をデータ主体に通知しなければならない⁶。

- ・ 情報の収集源
- ・ 管理者の名称及び住所
- ・ 収集の目的
- ・ データ主体から任意に提供されたか、義務的に提供されたか
- ・ データ主体が情報を提供できなかった場合の結果
- ・ 収集の法的根拠
- ・ 第三国又は国際機関に情報を移転する意図がある場合はその事実、及び、移転する当該第三国又は国際機関の個人情報の保護基準が十分であること
- ・ 情報の移転先
- ・ 情報の性質や種類
- ・ データ主体は、アクセス権、訂正権、個人情報の処理の拒否権、異議申立権を有すること
- ・ 情報規制当局の連絡先

また、これらの個人情報保護法に基づく義務に加えて、管理者は、情報アクセス促進法上、収集した個人情報へのアクセス方法等を記載したマニュアルを作成し、ウェブサイト上等において公表する義務も負う⁷。

² [2021年4月1日付 Guidance Note on Information Officers and Deputy Information Officers](#)5.1条。

³ 個人情報保護法 56条。

⁴ 個人情報保護法 55条1項及び個人情報保護規則 4条。なお、同規則 4条は 2021年5月1日より施行された。

⁵ 個人情報保護法 55条(2)及び [2021年4月1日付 Application form for Registration for Information Officers](#)。かかる登録のためのオンラインポータルサイトが開設されたが、当該ポータルサイトに問題が生じ登録期限は無期限延期とされ、情報規制当局は代替の登録手段を模索している。

⁶ 個人情報保護法 18条(1)及び(2)。

⁷ 情報アクセス促進法 51条(1)(b)、10条(2)(d)、51条(3)及び情報アクセス促進法に基づく規則案 5条(3)(c)。

ウ 個人情報の処理における義務

(i) 処理義務の概要

個人情報の処理は、個人情報保護法で定められた場合に限り行うことができ、それ以外は禁止される。具体的には、管理者は、(a)データ主体からの同意を得た場合、(b)データ主体が当事者である契約の履行のために必要な場合、(c)管理者に法的義務が発生している場合、(d)データ主体の正当な権利の保護のために必要な場合、(e)公法上の義務の履行のために必要な場合、又は、(f)管理者又は第三者の正当な利益を追求するために必要な場合に、それぞれ個人情報を処理できる⁸。

また、ダイレクトマーケティングを目的とする個人情報の処理を行う場合や、子供(18歳以下で、かつ、適格者(Competent Person)⁹による補助がなければ自らに関する行動や決定を行うことが法的にできない自然人¹⁰)の個人情報の処理を行う場合には、特別な方法等による同意が必要となる。具体的には、前者のダイレクトマーケティングを目的とする個人情報の処理については、データ主体からオプトイン方式(事前にデータ主体から所定の方式¹¹での同意を得る方法)により同意を取得する必要がある¹²、後者の子供の個人情報については、適格者の事前の同意が必要となる¹³。子供の個人情報の処理に係る情報規制当局による認可については、下記(ii)で詳述する。

また、個人情報保護法は、国外移転規制についても規定している¹⁴。具体的には、(a)国外における個人情報の受領者に、個人情報保護法と同様の処理義務を定めた拘束的企業準則又は拘束的契約に従わせた場合、(b)データ主体が個人情報の国外移転に同意している場合、(c)データ主体と管理者との間の契約の履行のために必要な場合、(d)データ主体の利益となる管理者と第三者との間の契約の履行に必要な場合、又は、(e)国外移転がデータ主体の利益になるが、データ主体から同意を取得することが合理的に見て可能でない場合のいずれかに該当する場合には、管理者はデータ主体の個人情報を国外移転できる。

(ii) 特別個人情報及び子供の個人情報の処理の認可

いわゆる「センシティブデータ」に相当する特別個人情報(Special Personal Information¹⁵)及び子供の個人情報に関しては、管理者がこれらの個人情報を処理することが原則的に禁止されている¹⁶。ただし、これらの個人情報の処理が、(a)公共の利益のために必要であり、(b)処理される個人情報について適切な保護措置が講じられている場合には、情報規制当局は、管理者に対し、これらのセンシティブデータに係る個人情報の処理を認可できる¹⁷。

この点に関し、情報規制当局は、2021年6月28日に、[特別個人情報及び子供の個人情報の処理に関する各ガイダンスノート](#)を公表し¹⁸、例えば、次のような記載がある。

- ・ 上記(a)の「公共の利益」は、個々人単位の利益ではなく、一般的に社会全体の利益となる場合を指す概念であり、公平及び

⁸ 個人情報保護法 11 条(1)各号。

⁹ 2021 年 6 月 28 日付 Guidance Note on Processing of Personal Information of Children(以下「子供の個人情報に関するガイダンスノート」という。)1.2 条では、Competent Person とは、“any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child”と定義されており、親権者などを指すものと思われる。

¹⁰ 子供の個人情報に関するガイダンスノート 1.1 条。

¹¹ 個人情報保護規則 Form 4 に同意書の雛形がある。

¹² 個人情報保護法 69 条。

¹³ 個人情報保護法 27 条(1)(a)及び 35 条(1)(a)。

¹⁴ 個人情報保護法 72 条。

¹⁵ 個人情報保護法 26 条。例えば、データ主体の宗教的・哲学的信念、人種・民族的出自、労働組合への加入、政治的主張、健康情報又は犯罪行為に関する情報が挙げられる。

¹⁶ 個人情報保護法 26 条及び 34 条。

¹⁷ 個人情報保護法 27 条(2)及び 35 条(2)。

¹⁸ 2021 年 6 月 28 日付 Guidance Note on Processing of Special Personal Information(以下「特別個人情報に関するガイダンスノート」という。)及び子供の個人情報に関するガイダンスノート。以下では、これらを合わせて「特別個人情報等に関するガイダンスノート」という。

正義の精神に基づきケースバイケースで判断されるべきである¹⁹。

- ・ 上記(b)の「保護措置」は、個人情報保護法 19 条で規定している安全保護措置(Security Safeguards)²⁰に準拠する必要がある²¹。
- ・ 情報規制当局は、子供の個人情報の処理に関して認可を与える際、管理者に対し、(ア)適格者の要請に応じて、適格者が子供の個人情報処理を評価したり、当該処理を拒否したりするための合理的な手段を提供すべき義務、(イ)処理する個人情報の性質、処理の方法、及び今後の処理方針を適格者に通知すべき義務、(ウ)目的達成のための必要性を超えた子供の個人情報の開示を控える義務、及び、(エ)子供から取得した個人情報の尊厳と秘匿性を保護するための合理的な手続を設定すべき義務など、合理的な条件を課すことができる²²。

(iii) 個人情報の処理に関する規制の免除

事業者は、個人情報の適法な処理のため、上記(i)の義務を履践しなければならないが、(a)情報規制当局より「個人情報保護法 37 条に基づく免除を与えられた場合」、又は、(b)「同法 38 条に定める「特定の機能(Certain Functions)」がある場合」には、かかる義務を遵守していなくても、個人情報の処理は適法となる²³。この点に関し、情報規制当局は、2021 年 6 月 21 日に、[個人情報処理に関する規制の免除についてのガイダンスノート](#)(以下「免除に関するガイダンスノート」という。)を発表した²⁴。

<上記(a): 個人情報の処理義務に違反していたとしても義務違反が免除される場合>

- ・ 上記(a)に関して、まず、管理者が個人情報の処理義務に違反していたとしても義務違反を免除される場合がある。個人情報保護法 37 条は、情報規制当局が当該免除をできる場合として、(ア)公共の利益が個人情報処理によるデータ主体の不利益を大きく上回る場合、又は、(イ)個人情報の処理がデータ主体や第三者の明らかな利益につながり、それによるデータ主体の不利益を大きく上回る利益を伴う場合を定めている²⁵。
- ・ そして、免除に関するガイダンスノートでは、「公共の利益」に含まれる内容を詳細化し、かつ、「公共の利益」に含まれるかはケースバイケースで判断されるべきだとし²⁶、免除の申請の際に管理者に対して、個人情報の処理がデータ主体に与える不利益よりも利益が大きく上回る理由を説明するよう要求している²⁷。また、当該ガイダンスノートでは、個人情報保護法 37 条による免除は、個人情報処理に係る規制の適用を全て免除するものではないことを明記している²⁸。

<上記(b): 特定の機能に基づく免除>

- ・ 上記(b)に関して、まず、特定の機能がある場合には管理者は個人情報保護法のいくつかの規定の適用を免除される。特定の機能の具体例としては、金融機関等の不誠実な行動に伴う経済的損失からデータ主体を保護するために管理者が個人情報の処理を行う場合が規定されており²⁹、個人情報保護法 38 条は、かかる場合には、個人情報保護法上のいくつかの規

¹⁹ 特別個人情報等に関するガイダンスノート 4.2.2 条。

²⁰ 個人情報保護法 19 条では、個人情報の不正アクセス等による損失を回避するため、個人情報に対するリスクを特定し、機密保持や情報保全を定めるなどのそのリスクに対する適切な安全手段を講じ、且つその安全手段を更新し続けることで、管理者は個人情報の秘匿性を守らなければならないと規定されている。

²¹ 特別個人情報等に関するガイダンスノート 4.2.2 条及び 4.3 条。

²² 子供の個人情報に関するガイダンスノート 5 条。

²³ 個人情報保護法 36 条。

²⁴ 2021 年 6 月 21 日付 Guidance Note on Exemptions from the Conditions for Lawful Processing of Personal Information in terms of Section 37 and 38 of the Protection of Personal Information Act 4 of 2013。

²⁵ 個人情報保護法 37 条(1)(a)及び(b)。

²⁶ 免除に関するガイダンスノート 4.2.3.3 条。

²⁷ 免除に関するガイダンスノート 4.2.4.2 条。

²⁸ 免除に関するガイダンスノート 4.2.5 条。

²⁹ 免除に関するガイダンスノート 4.3.3.1 条。

定の適用(例えば、データ主体が個人情報処理に反対する権利等)を免除されると定めている。

そして、免除に関するガイダンスノートでは、管理者に対し、個人情報の処理が個人情報保護法 38 条の適用により免除を受けるべき理由を説明するよう要求している³⁰。当該理由の説明は、情報規制当局による捜査を行ったときや管理者の行動評価を事後的に行うときに重要となる。

(3) データブリーチ時の管理者の対応

個人情報保護法上、データブリーチの明確な定義はないが、データ主体の個人情報がデータ主体が予め同意した提供先以外の者にアクセスされたなどの事情が存在すれば、情報の不正アクセス(Security Compromises)となり、データブリーチと考えられる。その場合、管理者は、情報規制当局及びデータ主体に対し、情報の不正アクセスの発見後、合理的な範囲で可能な限り速やかに、法執行の正当な必要性、又は、不正アクセスの範囲を決めるため及び管理者の情報システムの保全回復のために合理的に必要な手段を考慮して、通知しなければならない³¹。

後述の通り、サイバー犯罪法では、電子通信サービスプロバイダーや金融機関が管理者である場合には、かかる個人情報保護法上の通知義務が加重され、罰則も強化されることが見込まれる。

(4) エンフォースメント

個人情報保護法上、故意又は重過失により、管理者の同意なく、データ主体のアカウント番号を取得、開示、売却などの違法行為を行った者は、最大で 10 年以下の懲役又は罰金若しくはその両方が科される³²。この刑事訴追の代替として、情報規制当局は、1000 万南アフリカランド³³を超えない範囲で行政罰を課することができる³⁴。行政罰を受けた者は、情報規制当局と行政罰の分割払いの協議をするか、裁判所に不服申立てを行うことを選択できる³⁵。

また、データ主体又は情報規制当局は、個人情報の侵害につき、管理者に対し、損害賠償を求めて民事訴訟を提起できる³⁶。

3. 情報アクセス促進法

(1) 情報アクセス促進法の概要

情報アクセス促進法は、1994 年に南アフリカで初めて全人種参加型の総選挙が実施されてマンデラ政権が成立するまでの間、同国の法体系は長らく秘密主義的で権利の濫用を招くと批判されてきたことに対する反省を踏まえ、憲法上保護された情報アクセス権の実効性を高め、社会の透明性を向上すること等を目的として、2000 年に制定された。同法は、公的団体及び私的団体が保有する情報へのアクセスの手続を規定し、それぞれの団体に対し、収集した個人情報へのアクセス方法を記載したマニュアルの作成・公表義務を課している。前記 2.(2)イの末尾にも記載した通り、個人情報保護法と情報アクセス促進法の両方の適用を受ける事業者においては、両法に基づく義務が重畳的に課される。

³⁰ 免除に関するガイダンスノート 4.3.6 条。

³¹ 個人情報保護法 22 条。

³² 個人情報保護法 107 条、106 条(1)。

³³ 2021 年 8 月 23 日付け為替レート換算によれば、約 7177 万円。

³⁴ 個人情報保護法 109 条(2)(c)。

³⁵ 個人情報保護法 109 条(2)(d)。

³⁶ 個人情報保護法 99 条。

(2) 情報アクセス促進法に基づく規則案

冒頭 1.の②の通り、司法憲法開発省は、2021 年 4 月 23 日に、情報アクセス促進法に基づく規則案を発表し、パブリックコメントを募集した。規則の最終的な内容に関しては、パブリックコメントの結果を待つ必要があるが³⁷、同規則案では、情報アクセス促進法で課されていた義務が加重されている箇所があるので注意が必要である。例えば、アクセス希望者がアクセスを要求しなくても自動的に入手可能な記録の種類についての説明文に関して、南アフリカで個人情報を処理している事業者は、情報アクセス促進法では任意に担当大臣に提出することで足りたが³⁸、同規則案ではその前提としてその説明文をまとめて保管しなければならないという義務等が課されている³⁹。

4. サイバー犯罪法

(1) サイバー犯罪法の概要

冒頭 1.の③の通り、2021 年 5 月 26 日に、ラマポーザ南ア大統領の署名により、サイバー犯罪法が成立した。施行日は未定である。

同法は、サイバー犯罪に係る規制の枠組みや、サイバー犯罪の捜査権限に関する整備等を目的として制定された。同法は、ハッキングなどのデータに関する犯罪を明確化し、通信を受けとる人の財産又はその人自身に対する損害を発生させる電気通信を“Malicious Communications”として違法とした⁴⁰。また、手続面では、刑事手続法(Criminal Procedure Act)に加えて、警察当局に対し、データベース等の証拠を捜査・押収する権限を付与する旨を定め⁴¹、さらに、下記(2)に記載する通り、電子通信サービスプロバイダー及び金融機関に対し、一定のサイバー犯罪に関する通知義務を課す旨を定めている。

(2) 電子通信サービスプロバイダーや金融機関の通知義務

サイバー犯罪に際しては、サイバー犯罪に関する捜査の円滑化のため、個人情報保護法に基づく事業者の当局への通知義務及びデータ主体への通知義務が加重される予定である。具体的には、サイバー犯罪法では、電子通信サービスプロバイダーや金融機関に対して、特定のサイバー犯罪を認識するようになってから 72 時間以内に報告する義務を課しており⁴²、報告義務を怠り有罪判決を受けた場合、最高 5 万南アフリカランド⁴³の罰金が科せられる可能性がある。このように、個人情報を処理するなどして個人情報保護法の適用がある電子通信サービスプロバイダー及び金融機関は、サイバー犯罪法と個人情報保護法の両方の報告義務を課せられる場合があるので、両法律に基づく報告に関する手続やタイムラインをそれぞれ理解しておく必要がある。

5. まとめ

以上の通り、直近で個人情報保護法が実質的に全面施行され、その具体的細目が規定された規則やガイダンスノートが発表されたため、その内容を概説した。情報アクセス促進法に係る規則案やサイバー犯罪法は、今後の内容や施行日の確定が待たれるが、個人情報保護法による規制内容と重なる部分もあり、また、個人情報保護法で管理者に課された義務が加重されるものも存在するため、これらの法制に関係する事業者は、引き続き動向を注視の上、実務対応を進める必要がある。

以 上

³⁷ パブリックコメント募集は 2021 年 5 月 17 日に終了しているが、結果及び規則の最終的な内容の公表時期は未定である。

³⁸ 情報アクセス促進法 52 条(1)。

³⁹ 情報アクセス促進法に基づく規則案 5 条(1)。

⁴⁰ サイバー犯罪法 15 条。

⁴¹ サイバー犯罪法 27 条及び 28 条。

⁴² サイバー犯罪法 54 条(1)。

⁴³ 2021 年 8 月 23 日付け為替レート換算によれば、約 36 万円。

II 個人情報保護・データ保護規制 各国法アップデート

1. 日本

- 2021年7月1日、個人情報保護委員会は、「[PIAの取組の促進について—PIAの意義と実施手順に沿った留意点—](#)」を公表した。PIA(Privacy Impact Assessment、個人情報保護評価)は、個人情報等の収集を伴う事業の開始や変更の際に、プライバシー等の個人の権利利益の侵害リスクを低減・回避するために、事前に影響を評価するリスク管理手法である。PIAについては、民間の自主的な取組を促進することが望ましいとされている一方で、事業者に十分に浸透していない現状に照らし、今回、その意義や留意点が説明されている。
- 2021年7月19日、総務省は「DX時代における企業のプライバシーガバナンスガイドブック ver1.1」を[公表](#)した。企業がプライバシーガバナンスの構築のために取り組むべきことを取りまとめた ver1.0(2020年8月公表)に、実践的な参考事例が追加されたものである。具体的には、グローバルでプライバシーガバナンスを構築している事例や、従来は各組織ごとに有していた機能を一元化・統合する形でデータ・ガバナンス室を設置した事例等が追加されている。
- 2021年8月2日、個人情報保護委員会は「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、外国にある第三者への提供編、第三者提供時の確認・記録義務編、匿名加工情報編、認定個人情報保護団体編)の改訂版等を[公表](#)すると共に、これに関する意見募集結果を[公表](#)した。令和2(2020)年改正を踏まえた変更がなされている。

2. 中国

- 2021年7月28日、「最高人民法院による顔認識技術を使用し個人情報処理の民事事件の審理における法律適用に関する若干の問題の規定」が公布され、同年8月1日から施行された。本規定は、情報処理者が法律及び行政法規¹の規定又は訴訟当事者双方の間の約定に違反し、顔認識技術を使用して顔情報を処理したことに起因する民事事件において適用される司法解釈を人民法院(裁判所)が定めたものである。ホテル、商業施設、銀行、駅、空港、体育館等の事業所や公共施設において、法律及び行政法規の規定に違反し、顔認識技術を利用して顔認識、顔識別又は顔分析を行う行為などを、人民法院(裁判所)が、自然人の人格権の侵害に該当すると認めるべき行為として定めた。他方で、突発公共衛生事件²や、緊急状況において自然人の生命健康及び財産の安全保護に必要であるため顔情報を処理した場合などを免責事由として定めた。

3. 香港

- 2021年7月16日、Personal Data (Privacy) Ordinance の改正法案(以下「本法案」という。)が公布された。本法案は、同年7月21日に立法評議会に正式に提出され、審議に付されている。本法案では、データ対象者の同意を得ずに行われるドッキング行為(特定の損害を与える意図を持って、又は特定の損害が生じることについて注意を払わず漫然と、特定の人物の個人情報を、当該人物の同意なく、SNS や掲示板に晒す行為)を犯罪とするほか、個人情報保護委員会局長(プライバシー・コミッショナー)に、ドッキング行為による生成物の削除をプラットフォーム事業者等に命令する権限を与えるとともに、かかる命令への違反や捜査の妨害を付随的な犯罪として規定した。また、本法案では、プライバシー・コミッショナーに独自の刑事捜査及び起訴権限を与える。なお、本法案では、データ違反通知の義務化、データ処理業者の規制、データ保持義務、個人データの定義の拡大など、香港政府により2020年1月から継続的に議論されてきた他の修正案については触れられていないことから、今後の法案の動向が注目される。

¹ 行政法規は、国务院が憲法及び法律規定に基づき、法律規定を執行するため必要である行政法規事項、憲法第89条に定める国务院の行政管理職権に関する事項を定めたものである(憲法56条)。

² 突発公共衛生事件とは、突然発生した、社会の公衆の健康を著しく損害し又は損害する恐れのある重大な伝染病蔓延の状況、原因不明の集団的疾患、重大な食品及び職業の中毒並びにその他の公衆の健康を著しく影響する事件を指す(「突発公共衛生事件応急条例」2条)。

4. 米国

1. CCPA に関する FAQ のアップデート

2021 年 7 月 15 日、カリフォルニア州司法長官は、[CCPA に関する FAQ](#) を改定し、オンラインで個人情報を取得する場合、GPC シグナル³を通じた利用者によるグローバルなプライバシーコントロールが、オプトアウトを受付ける方法の一つに該当することが明確化された⁴。これにより、今後、関係する事業者はかかる方法によるオプトアウト権の行使を有効な権利行使として取り扱う必要がある。

2. CCPA Enforcement の実例サマリーの公表

2021 年 7 月 19 日、カリフォルニア州司法長官は、2020 年 7 月 1 日に同長官による CCPA の執行が開始して以降の当該執行に係る 27 件の実例の概要を[公表](#)した。州司法長官による CCPA の執行の場合は、CCPA に違反している旨の通知の受領から 30 日間の是正期間が用意されており(CCPA 1798.155(b))、同期間中に採られた対応策の概要も併せて公表されている。

以下では、掲げられた実例について、関係する業種、問題点及び具体的な事案の例を紹介する。掲げられた実例中、執行の対象となった業種としては、ソーシャルメディア関連や食料雑貨小売関連が比較的多いが、以下のとおり、マーケティング・広告プラットフォーム関連や、ゲーム、自動車、教育テクノロジー業界等を含め幅広く対象とされている。掲げられている CCPA 違反の問題点としては、プライバシーポリシーの不備や、「Do Not Sell My Personal Information」のリンクや個人情報の売却に係るオプトアウト手続の不備、個人情報の収集時の通知に関する不備といった、外観から発見し易い事由が数多く取り上げられている⁵。また、消費者の権利行使に関する情報提供の不備や、権利行使方法自体の不備も比較的多く取り上げられている。個人情報の売却を巡る規律の遵守に関連して、サービスプロバイダ契約の不備が併せて指摘されている例もある。

今回公表された実例はあくまで執行の実例のサンプルにすぎず、州司法長官による実際の執行の傾向は必ずしも明らかでないが、敢えて実例として公表していることから、州司法長官として特に注意喚起をしたいものを取り上げられているという趣旨とも考えられる。CCPA の適用を受ける日本企業は、州司法長官からの CCPA 違反の通知を受けるリスクへの対策として(なお、消費者による民事訴訟対策としても一定の効果があると思われる。)、掲げられた問題点を中心に、自社の CCPA 対応に不備がないか今一度確認しておくことが考えられる。

- 業種: オンラインマーケティングサービス、SNS、オンラインイベント販売、オンライン出会い系サービス、オンライン広告、オンラインプラットフォーム、オンラインゲーム、オンライン服飾小売等のオンラインビジネス、子ども用玩具販売、食料雑貨小売、ペット関連、家電等の小売業、マスメディア、エンターテインメント、自動車、教育テクノロジー、データベース/ディレクトリ販売等
- 問題点:
 - プライバシーポリシーの不備: 例えば、ある場面ではサービスプロバイダであるが、他の場面では事業者であるにもかかわらず、プライバシーポリシーにはそれに応じた適切な記載がなかった事案(なお、州司法長官からの通知を受けて行ったプライバシーポリシーの 1 度目の改定では、一般的な消費者には理解し難い難解な法律専門用語が含まれる等してかったため、2 度目の改定を行うことが求められた旨の記載もある)
 - 権限のある代理人制度に関する不備: 例えば、権利行使のために公証付証明の提出を求めていた事案、代理人による権利行使の方法についてプライバシーポリシーに記載していない等のプライバシーポリシー記載事項の不備に係る事案等
 - 「Do Not Sell My Personal Information」のリンクの不備: 単に「Do Not Sell My Personal Information」のリンクが欠け

³ CCPA に対応するべく、一部のインターネットブラウザに設けられた、データの売却の中止を求めるスイッチを指す。GPC については[こちら](#)も参照のこと。

⁴ B. REQUESTS NOT TO SELL PERSONAL INFORMATION(RIGHT TO OPT-OUT OF SALE)、7. What is the GPC?、8. How do I submit my opt-out request using the GPC?

⁵ なお、カリフォルニア州司法長官は、2021 年 7 月 17 日、カリフォルニア州の消費者が、事業者に対して、そのウェブサイト上に容易に発見できる形で売却しない旨のリンクを設置していない旨の通知を作成し易くする[ツール](#)を公開している。

ていたという事案のほか、例えば、運用する複数のウェブサイトそれぞれにおいて個人情報の売却に係るオプトアウトを希望する消費者に対して複数かつ別個のリクエストの提出を求めることとしていたり、「Do Not Sell My Personal Information」のリンクを各オンラインサイト上に表示していなかった事案、「Do Not Sell My Personal Information」のリンクを設置していたもののリンクが有効でなかった事案等

- 個人情報の売却・オプトアウト手続に関する不備：例えば、個人情報の売却に関しわかりにくい情報開示を行い、さらに、個人情報の売却に係るオプトアウトの手続を提供していなかった事案等
- 未成年者の個人情報の売却に関する不備：13歳～15歳の未成年者を含む利用者の個人情報に関して、未成年の利用者の個人情報についてのオプトイン、それ以外の利用者についてのオプトアウト手続を整備していなかった事案等
- サービスプロバイダ契約の不備：例えば、サービスプロバイダに対して契約で定められた事由以外での個人情報の開示等を禁止する規定を定めていなかった事案等
- その他には、消費者に対する通知の不備や金銭的インセンティブの通知の不備といった通知関連の不備のほか、権利行使方法の不備(消費者の権利行使に対する適時の対応の不備、有償での権利行使、ツールフリー番号の不備、認証の不備、認証のための事前のアカウント作成要求に関する不備等)も取り上げられていた。

5. 欧州

- ・ ルクセンブルクのデータ保護当局(CNPD)は、2021年7月16日、欧州連合(EU)の一般データ保護規則(GDPR)違反を理由に、Amazonの欧州法人(Amazon Europe Core S.à r.l.)に対して、GDPR違反を理由とする制裁金としては過去最高額となる7億4600万ユーロ(約970億円)の制裁金を科すことを決定した。Amazon.com, Inc.は、CNPDの決定は法的根拠を欠くとして争う姿勢を示している。決定文は公表されていないが、今回の決定は、フランスのプライバシー保護団体であるLa Quadrature du Net (LQDN)による2018年の告発を受けて開始された調査の結果を踏まえ、Amazonが利用者に対して実施するターゲティング広告がGDPRに違反していると認定したこと起因するものであると報道されている。
- ・ 欧州データ保護評議会(以下「EDPB」という。)は、2021年7月7日、2020年9月2日付けで承認されパブリックコメントに付された、GDPRにおける管理者と処理者に関するガイドラインを採択した。このガイドラインにおいては、管理者、処理者及び共同管理者の定義と、各役割に該当した場合の帰結について、詳細な解説がなされており、重要な指針を示すガイドラインとなっている。採択されたガイドラインの内容は、パブリックコメント版から大きく変わっていないものの、処理者との間で締結するデータ処理契約に規定すべき事項等、新たに明確化された点があることに留意する必要がある。
- ・ EDPBは、2021年7月7日、スマートフォン等の端末機器に搭載されている、利用者による音声コマンドを認識して実行する仮想音声アシスタント(Virtual Voice Assistants, 以下「VVA」という。))について、パブリックコメントの結果を踏まえた[ガイドライン](#)を公表した。同ガイドラインは、VVAの提供事業者が、一般データ保護規則(GDPR)及びe-Privacy指令を遵守するための留意点を示している。EUにおいてはVVAの利用実態が注目されており、今後、EU加盟国のデータ保護当局がVVAを調査・執行の対象としていくこととなるか注目される。
- ・ EDPBは、2021年7月7日、個人データの越境移転の枠組みの一つである行動規範(Code of Conduct)の採択プロセスや規定すべき内容に関する[ガイドライン](#)を公表した。行動規範は、EEA域内から域外へ個人データを移転する際の適切な保護措置の枠組みの一つとなり得るものであり、管理者や処理者が属するカテゴリーを代表する業界団体等が作成することができるものとして位置づけられている。将来的には、産業セクターごとの個別的なデータ処理のニーズに沿った越境移転の枠組みとして機能することが期待されている。

6. アラブ首長国連邦(UAE)

- ・ アブダビ首長国内に設けられたフリーゾーンのひとつであるAbu Dhabi Global Market(以下「ADGM」という。))において、2021年2月にデータ保護規則が改正され、基本的にGDPRと同水準の規制が導入されたことは、[当事務所個人情報保護・データ保護規制ニュースレター2021年3月29日号](#)でも紹介した。
- ・ 2021年7月25日、ADGMは、同月18日付で①[データ保護規則\(手数料\)規程\(Data Protection Regulations \(Fees\) Rules 2021\)](#)及び②[データ保護規則\(罰金\)規程\(Data Protection Regulations \(Fines\) Rules 2021\)](#)を制定したと公表した。これらの規程は、ADGM内に2021年2月14日時点で既に参入していた企業等については2022年2月14日、ADGM内に同日以降新規参入した企業等については2021年8月14日より発効する。
- ・ 2021年8月4日、ADGMは、上記の改正に関するウェビナーを開催し、データ保護庁が、近々、データ移転に関するEUの

標準的契約条項(Standard Contractual Clauses)と平仄を合わせた ADGM 標準的契約条項、データ保護規則のガイダンス並びにデータ保護影響評価及び適切なポリシー・ドキュメントのテンプレートを公表予定と発表した。ポリシー・ドキュメントのテンプレートは、英国の 2018 年データ保護法におけるアプローチと平仄を合わせたものとなることが予定されている模様である。

7. 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)が提出された。当該法案は、インドにおける個人情報の保護について包括的に定める初めての法案であるが、法案の内容を見直すため、国会合同委員会が当該法案に関する勧告報告書を国会に提出する予定とされている。当該報告書の提出期限は数度にわたり延長されているが、2021 年 7 月に 5 度目の延長がなされ、現時点では 2021 年 11 月から 12 月の国会で提出されることが予定されている。当該報告書提出の際に法案の改訂案が提出されるかどうかは公にされていないものの、当該報告書は法案内容に大きく影響を及ぼすものであると考えられるため、動向を注視する必要がある。

8. フィリピン

- 2021 年 8 月 4 日付で、National Privacy Commission より、International Organization for Standardization が公表しているデータ保護規格である ISO/IEC 29100、ISO/IEC 29151、ISO/IEC 24760 及び ISO/IEC 29134 に関する勧告が発表された。同勧告は、ISO の上記 4 規格がフィリピンの国家規格として認められる旨を確認するとともに、各組織に対して、プライバシー保護の枠組みの中で、同規格を採用するように求め、同規格の採用が Data Privacy Act of 2012 (Republic Act No. 10173)の遵守強化につながると定めている。なお、勧告中では、ISO 規格内で定められている、情報通信技術プロジェクトの組成、実施及び運用に際して検討するセキュリティメカニズムの説明がなされており、その中には、プライバシー影響評価の実施、個人情報保護の枠組みとリスク管理プロセスの確立、ID 情報の管理等に関する説明が含まれている。

9. ニュージーランド

- ニュージーランド政府は、2021 年 7 月 5 日、消費者データ権(Consumer Data Right)に関する新しい法的枠組みを実施することを**決定**した。政府は、2021 年中に、法令等を策定する役割を担う機関や、消費者データ権を行使するための方策を含め、消費者データ権の実行に関してさらなる決定をする予定である。また、消費者データ権は分野ごとに順次展開していくことが想定されており、今後、政府はどの分野において最初に消費者データ権の潜在用途を評価するかも検討する。2022 年には、消費者データ権を実施する法案が議会で提出される予定である。

10. ブラジル

- ブラジルの個人情報保護法(LGPD)における行政上の制裁に関する規定が、2021 年 8 月 1 日に施行された。LGPD 自体は 2020 年 9 月 18 日に施行されていたが、これにより、ブラジルのデータ保護当局(ANPD)は、LGPD に違反した個人情報取扱業者等に行政上の制裁を科すことができるようになった。行政上の制裁の具体的内容は以下の通りである。
 - 是正措置を講じるための期限を示してなされる警告
 - 一括制裁金。上限額は、ブラジル国内における当該法人又はそのグループ若しくはコングロマリットの売上高の 2%(税額を除く)、又は違反 1 件当たり 5,000 万ブラジルレアル(1 ブラジルレアル 20 円換算で 10 億円)のいずれか低い方
 - 日額の制裁金。合計額は、前記 2 の上限額を超えない範囲に限られる
 - 違反行為が正当に把握され、その発生が確認された場合、当該違反行為の公表
 - 違反状態が是正されるまでの間、当該違反行為に関連する個人データへのアクセス停止
 - 当該違反行為に関連する個人データの削除
 - 当該違反行為に関連するデータベースの運用を、最大 6 か月間部分的に停止(管理者の処理活動が是正されるまで、同じ期間の更新が可能)
 - 当該違反行為に関連する個人データのデータ処理を、最大 6 か月間停止(同じ期間の更新が可能)

9. データ処理に関連する活動の全部又は一部の禁止

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](#) 