西村あさひ法律事務所

ケニアのデータ保護法

個人情報保護・データ保護規制ニューズレター/アフリカニューズレター　2023 年 3 月 24 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 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　**ケニアのデータ保護法**／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 ケニアのデータ保護法

1. はじめに

ケニアでは、2019 年 11 月 25 日にデータ保護法(the Data Protection Act)が施行、2020 年 11 月にデータ保護法の遵守状況を確認する機関であるデータ保護委員会(the Office of the Data Protection Commissioner、以下「ODPC」という。)も設置され、その後、2021 年の終わりから 2022 年初めにかけて、同法に関する細則としての規則が制定及び施行された [1]。また、2022 年 6 月 14 日に、管理者(Data Controller)及び処理者(Data Processor)が ODPC に登録する手続きが開始された。

こうした近時の動向を受け、データ保護法が適用される事業者は、これら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。以下簡略に紹介する。

2. データ保護法

(1) 規制の概要

ケニアにおいて、個人データを保護する主な法令はデータ保護法であり、同法は、ケニアに所在するデータ主体の個人データを処理する事業者であれば、事業者がケニアに所在するか否かを問わず適用される。つまり、ケニアに事業拠点がない日本企業であっても、例えば、他社からケニアに所在する人の個人データの処理の委託を受けた場合には、理論的には同法の適用を受ける可能性がある。

適用対象となる事業者は、管理者又は処理者と呼ばれ [2]、管理者及び処理者には、同法上、主に、①データ・コミッショナーへの登録、②個人データ保護の基本原則の遵守、③データ主体への通知義務、④国外移転規制の遵守、⑤データ保護影響評価の実施が課される。また、同法では、データブリーチ [3]時において管理者が講じるべき対応等も規定されている。なお、同法に関する

[1] 具体的には、(i)the Data Protection (General) Regulations,2021(以下「データ保護に係る一般規則」という。)、(ii)the Data Protection (Compliance and Enforcement) Regulations, 2021、及び(iii)the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021(以下「登録に係る規則」という。)が挙げられる。

[2] データ保護法上、管理者は個人データの処理に係る目的・手段を決定する者をいい、処理者は管理者に代わり個人データを処理する者をいう(データ保護法 2 条)。

[3] データブリーチの意味については、後述 2(3)参照。

細則として、2021 年の終わりから 2022 年の初めにかけて、脚注 1 記載の規則が制定及び施行されている。

(2) 管理者及び処理者の義務

ア ①データ・コミッショナーへの登録

ODPC のトップであるデータ・コミッショナーは、データ保護法に基づき、登録が必要となる管理者及び処理者の基準を作成する [4]。当該基準は、対象となる事業、処理されるデータ数、処理されるデータに機微情報が含まれるか否かそのほかの条件を考慮して決定される [5]。当該基準に該当する管理者及び処理者は、登録に係るガイダンスノート [6]に従い、登録手続を行う必要がある。

イ ②個人データ保護の基本原則の遵守

データ保護法に基づき、管理者又は処理者は、下記の基本原則に従い個人データを処理しなければならない [7]。

- データ主体のプライバシー権を尊重して処理されていること
- 適法かつ公平に、いかなるデータ主体に対しても透明性のある方法で処理されていること
- 明白で特定された正当な目的で収集され、これらの目的と相容れない方法で処理されないこと
- 個人データが十分かつ関連性のあるものであり、処理の目的に必要な範囲に限定されていること
- 家族に関する情報又は私的事項を収集する場合には、一定の説明が行われること
- 個人データが正確であり、必要に応じて不正確な個人データが遅滞なく削除又は訂正され、アップデートされていること
- 収集した目的が存続するまでの間、データ主体を特定する書類を保管すること
- データ主体の同意、又は適切なデータ保護安全措置(adequate data protection safeguards)が講じられていることの証明がない場合、ケニア国外に移転しないこと [8]

ウ ③データ主体への通知義務

管理者又は処理者は、個人データを収集する際、データ主体に対し、上記②の基本原則に関する事項、データ保護法 26 条に規定するデータ主体の権利事項及び収集の目的等を通知することとされている [9]。

エ ④国外移転規制の遵守義務

管理者又は処理者は、(i)個人データ保護のため、適切なデータ保護安全措置が講じられた場合、(ii)データ・コミッショナーによる適切な決定が存在する場合、(iii)一定の目的のために国外移転を行う必要性がある場合、又は、(iv)データ主体の同意がある場合に国外移転を行うことができる [10]。なお、機微情報の国外移転に関しては、データ主体の同意及び適切な安全保護措置が講じられた場合にのみ認められる [11]。

---

[4] データ保護法 18 条。

[5] データ保護法 18 条(2)。なお、本ニューズレター発行時点の登録に係る規則及びガイダンスノートによれば、年間売上が 500 万ケニアシリング(2023 年 3 月 21 日付け為替レート換算によれば、約 506 万円。)以下であり、10 人以下の従業員の事業者の場合は原則免除されるが、通信、教育等の目的で個人データを扱う事業者は左記の免除要件にかかわらず登録義務を負うとされている(登録に係る規則 12 条及びガイダンスノート 4.参照)。もっとも、当該基準については、データ・コミッショナー等のケニア行政当局により変更される可能性があるため、都度確認されたい。

[6] Guidance Note on Registration of Data Controllers and Data Processors.

[7] データ保護法 44 条、25 条。

[8] データ保護法 25 条(h)、49 条(1)。

[9] データ保護法 29 条参照。

[10] データ保護法 48 条及び 49 条、データ保護法に係る一般規則 40 条。なお、個人データの国外移転が認められる事項の一つである(iii)「国外移転の必要性」に関しては、契約履行のために必要な場合や公共の利益のために必要な事項などに限られ、ODPC などのケニア行政当局の明確なコメントはないものの、欧州データ保護規則(GDPR)49 条と同様に、抑制的に適用されるべきと解されている。

[11] データ保護法 49 条 1 項、44 条、25 条(h)。

オ　⑤データ保護影響評価の実施

管理者又は処理者は、例えば、子供や社会的弱者(vulnerable groups)に係る機微情報の処理、遺伝データや生体認証データの処理及び個人データの大規模な処理等、データ主体の権利や自由に大きなリスクが生じ得る場合 [12]、データ保護影響評価(Data Protection Impact Assessment)を実施する必要がある。データ保護法 31 条(2)規定の評価基準及びデータ・コミッショナーが策定したデータ保護影響評価に係るガイダンスノート [13]に従い、管理者又は処理者は、データ保護影響評価を行う。データ評価影響評価レポートは、当該データ処理の 60 日前までに、データ・コミッショナーに提出されなければならない [14]。

(3)　データブリーチ時の管理者の対応

データ保護法上、「データブリーチ」とは、移転、保管その他の処理に係る個人データの不正な破壊、紛失、改変、権限のない開示につながるセキュリティ侵害を指す [15]。その場合、管理者は、データブリーチを認識してから 72 時間以内に遅滞なくデータ・コミッショナーに報告し、データ主体を特定できる場合には、合理的期間内に書面でデータ主体に通知しなければならない [16]。データ主体に対しては、データブリーチによる損害に対する保護手段を講じさせるため、データブリーチの内容、管理者又は処理者が行う予定の対処手段等を含む十分な情報を提供しなければならない [17]。

(4)　エンフォースメント

データ保護法に違反した者は、最大 300 万ケニアシリング [18]の罰金、又は 10 年以下の懲役若しくはその両方が科される [19]。その他、データ・コミッショナーは、(i)エンフォースメント通知(違反事実の通知や是正措置の要求等が記載された書面)及び(ii)行政罰としてのペナルティ通知を発出できるが [20]、これらに違反した者は、(i)の違反に関しては最大 500 万ケニアシリングの罰金、又は 2 年以下の懲役若しくはその両方が科され [21]、(ii)の違反に関しては最大 500 万ケニアシリングの罰金、又は違反者が企業の場合、年間売上の 1%のいずれか低い方が科される [22]。

また、損害を受けたデータ主体は、データブリーチにつき、管理者又は処理者に対して、民事訴訟で損害賠償請求ができる [23]。

3.　まとめ

以上の通り、近時でデータ保護法及び同法に関する細則としての規則が実質的において全面施行されたため、その内容を概説した。データ保護法が適用される事業者は、引き続き動向を注視する必要がある。

以　上

---

12 データ保護に係る一般規則 49 条。
13 Guidance Note on Data Protection Impact Assessment.
14 データ保護法 31 条(5)。
15 データ保護法 2 条。
16 データ保護法 43 条(1)及び(2)。
17 データ保護法 43 条(5)。
18 2023 年 3 月 21 日付け為替レート換算によれば、約 303 万円。
19 データ保護法 73 条。
20 データ保護法 58 条、63 条。
21 データ保護法 58 条(3)。
22 データ保護法 63 条。
23 データ保護法 65 条。

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

・　個人情報保護委員会は、2023 年 1 月 27 日を意見提出期限として「個人情報の保護に関する法律に係る EU 及び英国域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルールの一部を改正する告示（案）」の意見募集を行った。EU 又は英国域内から十分性認定に基づき提供を受けた個人情報を加工して得られた仮名加工情報の取扱いについて、既存の補完的ルールに規律を追加することを内容とする。

2.　韓国

・　2023 年 2 月 27 日、韓国の個人情報保護法(PIPA)の改正が成立した。今回の改正項目は、①個人情報の処理要件の緩和、②個人情報の国外移転に関する規律の変更、③映像情報処理機器規定の整備、④データ主体の権利の拡大等、多岐にわたり、2011 年に PIPA が制定されて以来の大幅な改正となる。その概要は個人情報保護・データ保護規制ニューズレター2023 年 3 月 10 日号を参照されたい。

3.　中国

・　2023 年 2 月 22 日、「個人情報保護法」に基づき、個人情報の権益を保護し、個人情報の越境活動を規範化するために、個人情報越境標準契約弁法が公布された。同法は本年 6 月 1 日施行予定である。個人情報取扱者が域外受領者と個人情報越境標準契約(以下「標準契約」という。)を締結することによって、中国域外に個人情報を提供する際は、本法が適用されることになる。標準契約を締結する方法で個人情報を中国域外に提供する場合、個人情報取扱者は、以下の 4 つの条件をすべて満たす必要がある(4 条)。
　①　重要情報インフラ運営者でないこと
　②　取扱いの個人情報が 100 万人未満であること
　③　前年 1 月 1 日以降に中国域外に提供した個人情報が累計して 10 万人分未満であること
　④　前年 1 月 1 日以降に中国域外に提供したセンシティブ個人情報が累計して 1 万人分未満であること
　また、個人情報取扱者は、中国域外に個人情報を提供する前に、事前に個人情報保護影響評価を行う必要がある(5 条)。
・　上記の標準契約及び個人情報保護影響評価は、標準契約の効力発生日から 10 営業日以内に、所在地の省レベルのインターネット情報部門に対して届出を行う必要がある(7 条)。

4.　香港

・　2023 年 2 月 9 日、PCPD(香港の個人情報保護委員会)は、Hong Kong Institute of Bankers の個人データ漏えい事案に関する検査報告書を公表した。同報告書によると、PCPD は、情報通信技術を利用して個人データを扱う組織に対して主に以下の事項を推奨している。
　・　定期的なリスク評価を行うことにより、ハッカー攻撃を防ぐために警戒を怠らないこと
　・　PDPO を遵守して個人データを使用し、保持し、かつ、個人データの全ライフサイクルを有効に管理するための個人データプライバシー管理プログラムの創設
　・　専任の役員のデータ保護責任者への任命
　・　可及的速やかに脆弱性へのパッチを適用するための有効なパッチ管理手続の作成を含む情報システムの管理を高めること
　・　データバックアップポリシーの策定及び重要なデータを含むシステムの定期的なバックアップを含む、データバックアップの定期的な実施
　・　サービスプロバイダを適切に管理すること

・　2023 年 2 月 20 日、香港の立法会において、PCPD は、個人データ（プライバシー）条例(PDPO)の実質的な改正を行うことを公表した。PCPD は、実質的な改正を 2023 年の上半期に行うことを示唆している。実質的な改正には以下の内容が含まれている。
　・　データ漏えいに関する通知の義務化：データを収集する者(「データユーザー」)は、「重大な危害の実際のリスク」がある場合、データ漏えいに気づいた時から 5 営業日以内に、PCPD 及び影響を受ける個人に、データ漏えいの通知をしな

ければならない
- 個人データの保持及びセキュリティの義務に関連する PDPO に基づくデータ処理者の直接規制の導入(現在、データ処理者のコンプライアンスを確保する責任は、当該処理者を使用するデータユーザーに課せられているため、データ処理者は PDPO の下で直接規制されていない)
- データユーザーが明確な個人データ保持ポリシーを策定することの義務化。ただし、PCPD は、特定の保存期間を規定するつもりはないとしている。
- (刑罰としての罰金を課す既存の権限に加えて)行政上の罰金を課す PCPD の明確な権限の追加。行政上の罰金の基準は、EU の GDPR と同様に、年間売上高をベースにする可能性もある。

5. 台湾

- 台湾個人情報保護法は、台湾における、非公務機関[24]による外国または中国大陸地区の域外第三者への個人情報の移転(以下、「個人情報越境移転」という。)について、原則としてこれを認めた上で例外的に禁止または制限する建付けを採用している(同法 21 条)。人力仲介業[25]の主務機関にあたる労働部は、前記の例外の一つである「移転先国において個人情報の保護についての十分な法規がなく、本人の権益が侵害されるおそれがあるとき」に該当するとして、2023 年 2 月 20 日から台湾における人力仲介業による中国大陸地区への個人情報越境移転を制限することを正式に公告した(労働発管字第 1120500319A 号公告)。

6. マレーシア

- マレーシアでは、2022 年 12 月 15 日、マレーシア個人情報保護局(Department of Personal Data Protection)が“Code of Practice on Personal Data Protection”を公表した。当該 Code は、個人情報保護法(PDPA)の主要な条項について、文言の意義や実務上の指針となるベストプラクティス等を説明している。

7. タイ

- タイでは、2023 年 2 月 10 日、個人情報保護委員会により、個人情報保護法の遵守に関する実務ガイドラインが公表された。当該ガイドラインでは、データ管理者・処理者向けに、個人情報保護法の適用範囲、同意取得の原則とその例外が適用される場面、政府機関等のよる個人情報の開示が認められる場面等について、具体的事例が紹介されている。
  Thailand: PDPC issues PDPA enforcement case study | News post | DataGuidance

8. 欧州

- 2023 年 1 月 17 日、欧州データ保護評議会(EDPB)は、Cookie Banner Task Force により作成された、一定の類型のクッキーバナーの ePrivacy 指令及び GDPR の適法性について整理したレポートを採択した。Cookie Banner Task Force は、NGO 団体である NOYB が、複数の EU 加盟国のデータ保護当局に提起したクッキー・バナーに関する 700 を超える苦情に、各 EU 加盟国間で整合的に対応するために 2021 年 9 月に設立されたものである。同レポートにおいては、特に、以下のようなクッキーバナーについて、違法の懸念があると指摘されている。
  - 同意ボタンがあるのに、同意を拒否するオプションが提供されていないクッキーバナー
  - あらかじめ「同意する」にチェックが入ったクッキーバナー
  - 同意するためのボタンはクッキーバナー上に表示されているものの、同意の拒否については、クッキーバナーの外にリンクを設置するにとどめる等、同意を拒否するための選択肢に利用者の注意を引くための視覚的なサポートが十分でないバナー
  - 必須でないクッキーの使用についてウェブサイト利用者の明確な同意を取得していない(ePrivacy 指令上の義務に違反)にもかかわらず、その後のデータ処理の GDPR 上の適法性根拠を「正当な利益」に求めるクッキーバナー
  - 同意の付与と同じ程度に容易にいつでも同意を撤回できるように設計されていないウェブサイト

---

24 台湾個人情報保護法における「非公務機関」とは、公務機関以外の自然人、法人その他の団体を指す(同法 2 条 8 号)。

25 ここでの「人力仲介業」とは、人力仲介業個人情報ファイル安全保護計画及び処理弁法 2 条に定められる、①就業サービス法 34 条により許可を得て設立された民間就業サービス機関、及び②障害者権益保障法 35 条 3 項により許可を得て設立された障害者就業サービス機関を指す。

9. 米国

・ 2023 年 3 月 15 日にコロラド州プライバシー法の施行規則がファイナライズされ公表された。同法が施行される 2023 年 7 月 1 日に施行される。また、カリフォルニア州では、カリフォルニア州プライバシー権法(CPRA)施行規則の最終案がカリフォルニア州プライバシー保護局(California Privacy Protection Agency)により承認されていたが(2023 年 2 月 7 日当事務所北米/個人情報保護・データ保護規制ニューズレター参照)、同最終案が、2 月 14 日にカリフォルニア州がカリフォルニア州行政法制局(Office of Administrative Law)に提出された。3 月 29 日までの期間レビューに付され、承認されれば 4 月 1 日に施行される。

10. ブラジル

・ 2022 年 12 月 23 日、ブラジルのデータ保護当局(ANPD)は、情報セキュリティインシデントの通知に関する新しいガイドラインを公表した。セキュリティインシデントがデータ主体に何らかのリスクを生じさせる又は重大な損害を与える可能性がある場合に通知が必要とされており、2023 年 1 月 1 日以降、同ガイドラインとともに公表されたセキュリティインシデント通知書(CIS)の新しい様式を使用しなければならない。
・ 同ガイドラインにより、(i)ANPD に直接インシデントを報告する義務は、データ管理者のみに課され、データ処理者には課されないことや、(ii)ANPD 及びデータ主体へのセキュリティインシデントの通知期限は、企業が当該インシデントを認識した時点から 2 営業日であること(但し、通知対象となるインシデントは内部的に確認されたものに限り、単なる疑いは含まれない)、(iii)2 営業日以内にインシデントについて十分な内容を通知できないことが正当化される場合には可及的速やかに、遅くとも最初の通知後 30 日以内に追加で通知しなければならないこと等が確認された。

11. オマーン

・ オマーンの個人情報保護法が 2022 年 2 月に公布されたことは、当事務所個人情報保護・データ保護規制ニューズレター2022 年 3 月 30 日号で取り上げたが、2023 年 2 月 13 日、同法が施行された。運輸・通信・IT 省(The Ministry of Transport, Communications, and Information Technology)が同法を補完する行政規則を制定することとなっているが、制定時期は未だ明らかにされていない。
・ 同法においては、同法の適用が除外される場合としてオマーンの経済的又は財政上の利益の保護のために必要な場合等が含まれるなど、欧州データ保護規則(GDPR)には見られない規定も存在する。同法の詳細は、当事務所中東ニューズレター2022 年 8 月 24 日号を参照されたい。

12. タンザニア

・ 2022 年 11 月 1 日、タンザニアで個人情報保護法第 11 号(The Personal Data Protection Act No.11 of 2022)が成立した。本法律は、情報通信及び IT 担当大臣が、本法律の施行開始日を定めた通達を発出した後に施行されるが、現時点で当該通達は発出されていない。本法律は、タンザニアにおける個人情報の収集と処理に関する最低限の規則を定めている。

西村あさひ法律事務所 広報室 E-mail