

外国における個人情報の保護に関する制度等の 調査結果報告書

2022年3月

アンダーソン・毛利・友常法律事務所 外国法共同事業

目次

第1章 総論.....	3
第2章 イスラエル国.....	4
第3章 カタール.....	10
第4章 コスタリカ共和国.....	18
第5章 チュニジア（チュニジア共和国）.....	25
第6章 パナマ.....	36
第7章 ペルー.....	43
第8章 南アフリカ（南アフリカ共和国）.....	51
第9章 モロッコ（モロッコ王国）.....	61
第10章 モンゴル.....	69

第1章 総論

I. 調査体制

本調査を実施するに当たっては、アンダーソン・毛利・友常法律事務所外国法共同事業（各国拠点を含む）及び同事務所からの再委託先となる各国・地域の法律事務所とが連携して、個人情報保護委員会の作成した所定の質問票に現地から回答を得る形で各国・地域における制度調査を行い、各国からの回答を基に本報告書を作成したものである。

II. 調査期間

2022年2月より同年3月10日までの期間、本調査を実施した。

III. 基準日

本調査の内容は、各国に質問票を配布した2022年2月15時点でのものであり、それ以降のアップデートについて網羅しているものではない。ただし、調査対象とする法令は、2022年4月1日時点で有効である法令、及び2021年12月17日までに制定された法令であって2022年4月1日より後に施行される予定のものとなっている。

IV. 調査対象国・地域一覧

本調査の対象となる国・地域は以下のとおりである。

1. イスラエル	2. カタール	3. コスタリカ共和国
4. チュニジア	5. パナマ	6. ペルー
7. 南アフリカ共和国	8. モロッコ	9. モンゴル

第2章 イスラエル国

I. 個人情報の保護に関する法制度

1. 個人情報の保護に関する法制度の有無

個人情報の保護に関する包括的な法令として、[プライバシー保護法 5741-1981](#) (Protection of Privacy Law, 5741-1981) (以下「プライバシー保護法」という。)が存在する。当該法令は、1981年3月11日に施行されている。

2. 1. 記載の法令に関する基本的事項

(1) 適用対象者

プライバシー保護法は、公的部門と民間部門のいずれにも適用される。同法は個人情報を保有又は処理するイスラエルの全ての事業体に適用される。

(2) 個人情報の定義

「データ」及び「センシティブデータ」に対して適用される。匿名データ及び法人に関するデータについては、同法の適用対象ではないと考えられる。

「データ」とは、個人の人格、地位、私事、健康状態、経済状況、職業上の資格、思想及び信念に関するデータと定義される (プライバシー保護法第7条)。

「センシティブデータ」とは、法務大臣が議会委員会の承認を得て指定した個人の性格、親密な状況、健康状態、経済状況、思想及び信念等に関するデータをいう。ただし、本報告書作成時点ではそのような指定はされていない (プライバシー保護法第7条)。

(3) 地理的適用範囲

イスラエルの法律は、域外適用が法律に明示的に規定されているか、又は法律の言語と目的から暗示されていない限り、同国内に適用される。域外適用の決定がなされない限り、プライバシー保護法の管轄権はイスラエル国内の行為に限定されると想定される。

3. 留意点

イスラエル人の個人情報を取り扱う外国法人にプライバシー保護法が適用されるか否かは、未解決の法的問題である。以下を含むイスラエルとの様々なつながりの全体的な強さに基づき、プライバシー保護法が適用される可能性がある。したがって、下記のとおりつながりの強さ次第で、イスラエル国外に所在するデータ主体の個人データに対しても、プライバシー保護法が適用され得る。

- (i) データ主体がイスラエルに所在するか
- (ii) 個人データを含むサーバーがイスラエルに所在するか
- (iii) 個人データの管理者がイスラエルの事業体であるか、その活動に関与しているイスラエルの関連会社があるか

(iv) イスラエルで処理活動が行われているか

II. 当該外国の個人情報の保護に関する制度についての「一定の指標」となり得る情報の有無

イスラエルは、EU の十分性認定を 2011 年 1 月 31 日に取得した。

III. 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及び本人の権利に関する法令規定の有無

II 記載のとおり、イスラエルは EU の十分性認定を取得している国であるため、本項目は記載していない。

IV. 域内での保有・保管等の義務及びガバメントアクセス

1. データ・ローライゼーション規制 ①域内での保有・保管義務

個人情報・個人データを域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令¹においては、現地法律事務所が把握している限り、存在しない²。

2. データ・ローライゼーション規制 ②域外移転の制約による実質的な域内保持義務

個人情報・個人データの域外移転を制約することにより実質的に域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令³においては、現地法律事務所が把握している限り、存在しない。

3. ガバメントアクセス

ガバメントアクセスを根拠づける法令として、[刑事訴訟規則（拘留及び捜索）-1969](#) (the Criminal Procedure Ordinance (Detention and Search)-1969) (以下「刑事訴訟規則」という。)、[一般安全保障法 2000](#) (General Security Service Law-2000) (以下「シャバク法」という。)、[盗聴法-1979](#) (the Wiretapping Law-1979) (以下「盗聴法」という。)がある。これらのうち刑事訴訟規則に基づくガバメントアクセスは、原則として裁判所の令状を得て行われるため、ここではシャバク法及び盗聴法を紹介するものとする。シャバク法及び盗聴法の調査項目別の概要は以下のとおりである⁴。

¹ 代表的か否かに関する判断は現地法律事務所が行っている。

² 事業セクター（銀行、金融、健康、政府等）によっては、関連するデータ・ローライゼーションに関する要件が存在する可能性はあるが、ケースごとに検討すべき問題である。

³ 代表的か否かに関する判断は現地法律事務所が行っている。

⁴ その他ガバメントアクセスに関する規定が設けられる可能性のある法律として、

(1) 法的根拠

ア 目的

シャバク法上、政府アクセスの目的は特定されていない。

盗聴法上、首相は、国家安全のために必要であると判断した場合に、国家安全のための秘密監視の許可を出すことができる（盗聴法第4条）。また、地方裁判所の長は、行為を防ぎ又は行為を検知するために必要であると判断した場合に、法執行のための秘密監視の許可を出すことができる（盗聴法第6条）。

イ 実施主体

シャバク法は、裁判所命令を必要とするのではなく、権限はイスラエルの国家保安局 (Israeli Security Service) にある。

盗聴法は、国家安全保障上の権限は、首相 (Prime Minister) 及び防衛大臣 (Minister of Defense) に与えられる。法の執行については裁判所の命令、又は、特定の状況下においては、イスラエル警察長官 (General Commissioner of the Israel Police) に与えられる。

ウ 取得される個人データの種類に関する限定の有無・概要

シャバク法及び盗聴法ともに、取得される個人データに制限はない。

エ 制限規定の有無・概要

シャバク法では、12時間を超える公共の建物内での活動は、建物所有者の許可及び裁判所の命令を必要とする（シャバク法第8条(c)）。

盗聴法では、国家安全保障のための通信傍受許可については、特定の防衛施設職員だけが許可を受けることができる。また、裁判所命令がない限り、特定の種類の特権的な会話（法律顧問と依頼人との間の会話等）の盗聴は一般的に制限されている。

オ 手続規定の有無・概要

シャバク法に基づくガバメントアクセスには、国家保安局局長の許可が必要であり、また、当該許可に関する報告義務も存在する。

盗聴法に基づくガバメントアクセスについては、国家安全保障目的でのアクセス、法執行のための裁判所命令によるアクセスそれぞれについて、報告義務が存在する（盗聴法第4条及び第6条）。さらに、いずれのガバメントアクセスの許可・命令

[サイバー防衛及び国家サイバー総局法草案（サイバー防衛を強化する権限）（暫定条項）-2021](#) (Cyber Defense and National Cyber Directorate Law (Authority to Strengthen Cyber Defenses) (Temporary Provision)-2021) が存在するが、現在は草案段階であり、制定されていない。

についても、3ヶ月の期間制限が存在するが、更新可能である。やむを得ない事情がある場合には、国家安全保障目的、法執行目的いずれの場合も、48時間の緊急許可を発出することができる（盗聴法第5条及び第7条）。

(2) 正当な目的の追求

シャバク法上ガバメントアクセスを目的に必要な範囲に限る規定は存在しない。

盗聴法上、首相は、国家安全のために必要であると判断した場合に、国家安全のための秘密監視の許可を出すことができる（盗聴法第4条）。盗聴法上、地方裁判所の長は、行為を防ぎ又は行為を検知するために必要であると判断した場合に、法執行のための秘密監視の許可を出すことができる（盗聴法第6条）。

(3) 承認の要求

ア 事前承認及び事後承認、保護措置

上記（1）イ及びオ記載のとおり。

イ 暗号復号強制、保護措置

暗号復号強制に関して規定した法令は特にない。

(4) 取得された個人データの取扱いに対する制限

ア 保管期間の定めの有無・概要

一般的には、ガバメントアクセスに関する許可又は命令に従って保管することとなる。また、盗聴法では、個人データを含む資料が必要でなくなった場合までが保管期間となる（盗聴法第9条b）。

イ データの取扱者に関する制限、保護措置

一般的には、ガバメントアクセスに関する許可又は命令に従って保管することとなる。

ウ 安全管理措置に関する定めの有無・概要

一般的には、ガバメントアクセスに関する許可又は命令に従うこととなる。また、盗聴法では、資料をいかに消去するべきかに関する法令が存在する（盗聴法第9条b及び関連する法令）。

(5) 透明性

ア ガバメントアクセスの事実の通知義務の有無・概要

シャバク法及び盗聴法では、個人情報主体及び個人情報の保有者に対する通知は行われない。

イ ガバメントアクセスの実施状況の公表・公的機関に対する報告

シャバク法では、行政機関への報告義務がある（シャバク法第12条）。盗聴法では、立法部であるクネセットサブコミッティー（Knesset Subcommittees）への報告義務がある（盗聴法第4条）。

ウ 監督機関による監督状況の公表

特になし。

(6) 監督・調査・審査の仕組み

ア ガバメントアクセスの実施に対する監督・調査・審査の仕組みを規定する法令の有無・名称

各法律に基づく規制当局はイスラエルの行政法において規制されており、従って、イスラエル司法当局に従うこととなる。

シャバク法は、政府連合（government coalition）による広範な監視を創出する省庁間委員会（inter-ministerial committee）への報告を義務付けており、また、内部監査人の任命も規定している。

イ 監督機関の名称・権限・独立性・長の任命プロセスと身分保障

上記ア記載のとおり。

ウ 調査形態

監督機関は、報告を受け、これについて審議することができる。実地検査に関する言及は存在しない。

エ 監督メカニズムの実効性を評価する仕組み・監督機関による公表の制度

特になし。

(7) 救済

ア 違法なガバメントアクセスに対する救済制度の有無・救済の内容・訴訟の結果を遵守する法的義務・救済手続の公表

シャバク法及び盗聴法のいずれにも、固有の救済制度の定めはない。もっとも、イスラエルにはいくつかの不法行為法が存在しており、国家は民事責任の対象として私企業として扱われ得る（特に民事不法行為法（国家責任）（the Civil Tort Law

(Liability of the State)-1952))。もともと、法律に基づいて行動する場合を含む責任

免除制度が存在するため、不法行為法に基づき解決されるのは、法律に違反する行為が行われた場合である。

イ 救済を提供する行政機関・裁判所

上記ア記載のとおり。

ウ 外国人の救済の可否

一般論として、外国人が、イスラエルにおいて不法行為等に基づく訴訟を提起することは可能である。

エ ガバメントアクセスによって取得された情報に基づき訴追された者の権利

上記ア記載のとおり。

V. データ保護機関の有無及び連絡先

The Privacy Protection Authority

(https://www.gov.il/en/departments/the_privacy_protection_authority/govil-landing-page%20)

電話 : +972 073 3928555

電子メール : ppa@justice.gov.il

第3章 カタール国

I. 個人情報の保護に関する法制度

1. 個人情報の保護に関する法制度の有無

個人情報の保護に関する包括的な法令として、[個人情報の保護に関する 2016 年法律第 13 号](#) (Law No. 13 of 2016 Concerning Personal Data Protection) (以下「個人情報保護法」という。)が存在する。当該法律は、2016 年 12 月 31 日に施行されている。

2. 1. 記載の法令に関する基本的事項

(1) 適用対象者

個人情報保護法は、公的主体にも民間主体にも適用される。

(2) 個人情報の定義

個人情報保護法は、「個人データ」と「機密情報」を規制している。

「個人データ」は、個人に関する情報のうち、当該データ自体又は他のデータとの組み合わせによって個人を識別可能なものと定義している(個人情報保護法第1条)。

「機密情報」とは、人種、子供、健康、身体的又は精神的状態、宗教的信条、夫婦関係、犯罪に関するデータと定義されている(個人情報保護法第16条)。

(3) 地理的適用範囲

個人情報保護法は、カタール国内で行われる処理活動(収集を含む。)に対して適用される。そのため、本人がカタールに所在しているか否かによって適用が決まるわけではない。

II. 当該外国の個人情報の保護に関する制度についての「一定の指標」となり得る情報の有無

カタールは、EU の十分性認定を取得しておらず、また具体的な取得等に係る手続はなされていない。

また、APEC の CBPR システムには加盟しておらず、また具体的な加盟等に係る手続はなされていない。

III. 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及び本人の権利に関する法令規定の有無

1. 収集制限の原則 (Collection Limitation Principle)

(1) 規定の存否と概要

個人情報保護法には、収集制限の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 適法かつ公正な手段による取得その他収集の制限を定めた規定

個人情報保護法に基づき、個人データの取扱いは、以下のような要件に従う。(ア) 個人データの取扱いは、透明性、誠実性、人間の尊厳の尊重及び適正慣行の原則と整合的であること（個人情報保護法第3条）、(イ) 管理者は、データ主体の個人データを処理する前に、データ主体に対し一定の情報を提供すること（個人情報保護法第9条）、(ウ) 管理者は、収集された個人データが関連性があり、収集の目的に適切であり（また、正当でなければならない。）、かかる目的を達成するために必要な期間を超えて保持されてはならない（個人情報保護法第10条）。

イ 取得に際してのデータ主体への通知又はデータ主体からの同意取得を定めた規定

管理者は、個人データ主体の個人データを処理（収集を含む。）する前に、個人データ主体の同意を得なければならない。ただし、管理者又はデータの送信先である第三者の正当な目的を達成するために処理が必要な場合は、この限りでない。黙示的又は推定的同意は、個人情報保護法の下では明示的に許可されていないため、同意は「明白で、明示的かつ自由に与えられ」なければならない。管理者は、機密性の高い個人データを処理する前に、CDP から許可を取得する必要がある。管理者は、個人データを処理する前に、次の情報をデータ主体に提供しなければならない。(ア) 個人データを処理又は利用する管理者又はその他の者のための情報を特定すること、(イ) 個人データを処理するための管理者の正当な目的、(ウ) 処理アクティビティの説明、(エ) 管理者が個人データを第三者に開示するか否か、(オ) 個人的なデータ処理が法律を遵守するために必要なその他の情報（個人情報保護法第9条）。

(2) 当該原則が実質的に及ばない分野等について

管理者は、次の場合には、個人データ主体の同意なく個人データを処理することができる。(ア) 管理者又は第三者の正当な目的を達成するために必要な場合、(イ) 公益であり、法律と一致している場合、(ウ) 法的義務又は裁判所命令と一致する場合、(エ) 個人の重要な利益を守る場合、(オ) 公共の利益のための科学研究に関連する場合、(カ) 犯罪捜査に関連する場合（個人情報保護法第4条、第19条）。

2. データ内容の原則（Data Quality Principle）

個人情報保護法には、データ内容の原則又はこれに対応する事業者・機関の義務に

関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

ア 利用目的に関連する限度での取扱いを定めた規定

管理者は、収集された個人データが管理者の正当な収集目的に関連し、適切であり、かつ、更新されていることを検証する。管理者は、正当な収集目的を達成するために必要な期間に限り、個人データを保持する（個人情報保護法第10条）。

管理者は、処理者が正当な収集目的及び個人情報保護法に従って個人データを処理していることを確認する（個人情報保護法第12条）。

イ 利用目的の達成に必要な範囲内における正確性の確保を定めた規定

上記ア参照。

(2) 当該原則が実質的に及ばない分野等について

特になし。

3. 目的明確化の原則（Purpose Specification Principle）

個人情報保護法には、目的明確化の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

ア 取得時又はそれより前の個人データの利用目的の特定を定めた規定

管理者は、個人データを処理する前に、個人データを処理するための管理者の正当な目的を個人データ主体に提供しなければならない（個人情報保護法第9条）。

イ 特定された利用目的又は当該利用目的と矛盾しない目的の範囲内における利用を定めた規定

管理者は、目的の達成のために必要な範囲に限り、個人データを保持しなければならない（個人情報保護法第10条）。また、管理者は、処理者が正当な収集目的及び個人情報保護法に従って個人データを処理していることを確認する（個人情報保

護法第 12 条)。

ウ 利用目的の変更時における利用目的の特定を定めた規定

個人データ主体は、個人データが収集される前にその目的を知らされなくてはならず、また、個人データ主体は個人データを処理すること及び処理の目的を通知されなくてはならない（個人情報保護法第 6 条及び第 9 条 (2)）。したがって、個人データの処理の目的が変更された場合には、管理者は当該変更につき個人データ主体に通知しなければならない。

(2) 当該原則が実質的に及ばない分野等について

特になし。

4. 利用制限の原則 (Use Limitation Principle)

個人情報保護法には、利用制限の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

ア あらかじめ特定した利用目的の範囲を超えて開示すること又は利用可能な状態に置くことを制限する規定

管理者は、個人データを第三者に提供する場合、個人データ主体の同意を取得しなければならない。また、個人データの管理者は、個人データを利用目的達成に必要な期間を超えて保有してはならない（個人情報保護法第 10 条）。さらに、個人データの利用目的が既に満たされた場合、個人データ主体は、個人データの削除又は消去を請求する権利をもつ（個人情報保護法第 5 条 (3)）。

イ あらかじめ特定した利用目的の範囲を超えてその他の利用を制限する規定

上記アのとおり。

(2) 当該原則が実質的に及ばない分野等について

特になし。

5. 安全保護の原則 (Security Safeguards Principle)

個人情報保護法には、安全保護の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

管理者及び処理者は、個人データを保護し、個人データの開示、個人データへの違法又は偶発的なアクセス若しくは使用を防止するために、適切な管理上、技術上及び財務上の予防措置を講じなければならない（個人情報保護法第 8 条第 3 項及び第 13 条）。

(2) 当該原則が実質的に及ばない分野等について

該当なし。

6. 公開の原則 (Openness Principle)

個人情報保護法には、公開の原則又はこれに対応する事業者・機関の義務に関する規定が一部存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

ア 個人データの取扱いに関する方針の策定に関する規定

管理者は、個人データを効果的に管理するための社内ポリシーと手順を確立する（個人情報保護法第 11 条第 5 号）。

イ 個人データの存在と性質、主な利用目的、管理者の identity や所在地を容易に認識できる方法による提供に関する規定

該当なし。

(2) 当該原則が実質的に及ばない分野等について

特になし。

7. 個人参加の原則 (Individual Participation Principle)

個人情報保護法には、個人参加の原則又はこれに対応する事業者・機関の義務に関する規定が一部存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

ア 自己に関する個人データの開示を求める権利を定める規定

個人データ主体は、手数料を支払い個人データのコピーを取得することができる(個人情報保護法第6条)。

イ 自己に関する個人データの消去、訂正、完全化又は変更を求める権利を定める規定

個人データ主体は、次の権利を有する。(ア) 個人データを含む取扱活動及び取扱いの目的を知る、(イ) 不正確な個人データの開示について知る、(ウ) 手数料を支払い個人データのコピーを取得する、(エ) 収集目的を達成するために処理が不要である場合、又は、過度、差別的、不公正、若しくは違法に個人データが取扱われている場合に、異議を述べる(個人情報保護法第5条、第6条)。

個人データ主体は、次の場合に、個人データの削除を要求することができる。(ア) 個人データ主体が取扱いに対する同意を撤回した場合、(イ) 収集目的を達成するために処理が不要である場合、(ウ) 個人データの取扱いが過度、差別的、不公正、又は違法である場合、(エ) 処理の目的が達成された場合、(オ) 管理者が個人データを保有する正当な理由がない場合(個人情報保護法第5条)。

個人データ主体は、個人データ又はプライバシーに重大な個人的損害を引き起こす可能性があるデータ侵害について通知を受ける権利を有する(個人情報保護法第14条)。

ウ 権利行使ができない場合の理由の通知や異議申し立てを定める規定

該当なし。

(2) 当該原則が実質的に及ばない分野等について

特になし。

8. 責任の原則 (Accountability Principle)

個人情報保護法には、責任の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

運輸通信省 (The Ministry of Transport and Communications) は、苦情を調査し、管理者及び処理者に個人情報保護法違反の是正を求める拘束力のある決定を下すことができる。同省は、違反の性質に応じて 100 万 QR 又は 500 万 QR までの罰金を科すことができる (個人情報保護法第 23 条、第 24 条)。同省は、個人が法人の名において又は法人のために個人情報保護法に違反した場合、100 万 QR の追加の罰金を課すことができる (個人情報保護法第 25 条)。

(2) 当該原則が実質的に及ばない分野等について

特になし。

IV. 域内での保有・保管等の義務及びガバメントアクセス

1. データ・ローカライゼーション規制 ①域内での保有・保管義務

個人情報・個人データを域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令⁵においては、現地法律事務所が把握している限り、存在しない。

2. データ・ローカライゼーション規制 ②域外移転の制約による実質的な域内保持義務

個人情報・個人データの域外移転を制約することにより実質的に域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令⁶においては、現地法律事務所が把握している限り、存在しない。

⁵ 代表的か否かに関する判断は現地法律事務所が行っている。

⁶ 代表的か否かに関する判断は現地法律事務所が行っている。

3. ガバメントアクセス

ガバメントアクセスを根拠付ける法令として、サイバー犯罪防止法、電気通信法が挙げられるが、捜査を行うには裁判所の令状が必要であり、我が国の制度と比較して、カタールへの個人データの越境移転に伴い当該個人データに係る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とは解されないことから、本報告書には記載しない。

V. データ保護機関の有無及び連絡先

The Compliance and Data Protection Department (www.motc.gov.qa/en)

電話 : +974 4045 1111

電子メール : info@motc.gov.qa

第4章 コスタリカ共和国

I. 個人情報の保護に関する法制度

1. 個人情報の保護に関する法制度の有無

個人情報の保護に関する包括的な法令として、[個人情報処理に関する人の保護に関する法律](#) (Law on the Protection of Persons Regarding the Processing of their Personal Data No. 8968 of 2011) (以下「個人情報保護法」という。)が存在する。個人情報保護法は2011年9月5日に施行された。また、[行政命令](#) (Executive Decree No. 37554-JP of 30 October 2012 Regulating Law No. 8968, as amended by Decree No. 40008-JP of 2013) (以下「行政命令」という。)が存在する。行政命令は2013年3月5日に効力が発生し、2016年12月6日に改正された。

2. 1. 記載の法令に関する基本的事項

(1) 適用対象者

公的部門と民間部門のいずれも対象とする。地方自治体も適用対象となる。

ただし、以下の例外がある。

まず、金融機関には適用されない。

また、内部、個人又は家庭でのみの使用のために保有され、管理されているデータベースについては、適用されない。ただし、当該データベースが販売又は取引されている場合にはこの限りではない。

さらに、以下に関する事項については、個人情報保護法の権利及び原則は適用されない。

(ア) 国家安全保障、(イ) 保安及び公権力の行使、(ウ) 犯罪の予防、起訴、捜査、拘禁、抑圧、あるいは懲戒処分、(エ) 個人の身元が危険にさらされていない場合の、統計的、歴史的又は科学的調査目的でのデータベースの運用、(オ) 公共サービスの適切な提供、(カ) 公的機関によって行われる行政の効果的な通常の活動。(個人情報保護法第2条、第8条及び第9条(4))

(2) 個人情報の定義

「個人データ」は、特定された又は特定可能な個人に関するあらゆるデータと定義される(個人情報保護法第3条(b))。

「センシティブデータ」は、人種的起源、政治的見解、宗教的又は精神的信念、経済状態、生物医学的又は遺伝学的情報、性的指向等を含む個人に密接した情報をいう(個人情報保護法第3条(e))。

さらに、「保有者」(holder)とは、解剖学的、生理学的、精神的、経済的、文化的又は社会的アイデンティティによって直接又は間接にそのアイデンティティが決定される者をいうと定義される(行政命令第2条)。

(3) 地理的適用範囲

コスタリカ共和国内に所在するデータベースをもつ個人又は企業にのみ適用され

る。個人情報主体がコスタリカ共和国内に所在するか否かは問わない。域外適用に関する特定のルール及び判例法はない。

3. 留意点

個人情報保護法を改正する法律が、2021年2月12日に特許商標公報で発布された。法報告書作成段階において、議会で審議中である。

II. 当該外国の個人情報の保護に関する制度についての「一定の指標」となり得る情報の有無

コスタリカは、EU の十分性認定を取得しておらず、具体的な取得等に係る手続もなされていない。

また、APEC の CBPR システムには加盟しておらず、具体的な加盟等に係る手続もなされていない。

III. 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及び本人の権利に関する法令規定の有無

1. 収集制限の原則 (Collection Limitation Principle)

(1) 規定の存否と概要

個人情報保護法には、収集制限の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 適法かつ公正な手段による取得その他収集の制限を定めた規定

個人データを取得する場合、保有者は、データベースの存在及び目的、受領者、必須又は選択ベースであるか、データの取扱い、データの提供を拒否した場合の帰結、権利を行使する可能性、並びにデータベースの管理者の身元及び住所について、事前に明示的、正確かつ明確に通知されなければならない。事前の同意は物理的又は電子的手段のいずれかにより書面で取得されなければならない。当該同意はいつでも撤回することができる。かかる同意は、管轄権を有する司法当局又は議会の特別調査委員会により命令が出された場合、データが一般に公開されている場合、又はデータが法律により提供されなければならない場合には適用されない（個人情報保護法第5条及び第6条（4）並びに行政命令第4条、第5条及び第12条）。

イ 取得に際してのデータ主体への通知又はデータ主体からの同意取得を定めた規定

上記ア記載のとおり。

(2) 当該原則が実質的に及ばない分野等について

特でない。

2. データ内容の原則 (Data Quality Principle)

個人情報保護法には、データ内容の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

ア 利用目的に関連する限度での取扱いを定めた規定

個人データが、最新の、真実の、正確な、かつ収集された目的に十分なものである場合のみに、取得され、保存され、又は、自動化され若しくは手動の処理のため利用される（個人情報保護法第6条）。

イ 利用目的の達成に必要な範囲内における正確性の確保を定めた規定

上記アのとおり。

(2) 当該原則が実質的に及ばない分野等について

特でない。

3. 目的明確化の原則 (Purpose Specification Principle)

個人情報保護法には、目的明確化の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

ア 取得時又はそれより前の個人データの利用目的の特定を定めた規定

個人データの取得前に利用目的を特定し、特定された利用目的の範囲内又は当該利用目的と矛盾しない範囲内で利用し、利用目的が変更された場合には変更後の利用目的を特定しなければならない（個人情報保護法第5条及び第6条、並びに行政命令第21条）。

イ 特定された利用目的又は当該利用目的と矛盾しない目的の範囲内における利用を定めた規定

上記アのとおり。

ウ 利用目的の変更時における利用目的の特定を定めた規定

上記アのとおり。

(2) 当該原則が実質的に及ばない分野等について

当該原則に特定した例外規定はない。ただし、一般的例外に該当する場合には、当該原則の適用はない。

4. 利用制限の原則 (Use Limitation Principle)

個人情報保護法には、利用制限の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

ア あらかじめ特定した利用目的の範囲を超えて開示すること又は利用可能な状態に置くことを制限する規定

個人情報主体の同意がある場合を除き、開示や提供、及びあらかじめ特定された利用目的の範囲を超えたその他の利用ができない（個人情報保護法第 11 条）。

イ あらかじめ特定した利用目的の範囲を超えてその他の利用を制限する規定

上記アのとおり。

(2) 当該原則が実質的に及ばない分野等について

特にない。

5. 安全保護の原則 (Security Safeguards Principle)

個人情報保護法には、安全保護の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

個人データを収集又は管理する個人又は事業者は、一般的な手順及び手続に関する行動のセキュリティプロトコルを実装しなければならない。また、当該プロトコルは、Agencia de Protección de datos de los Habitantes(以下「PRODHAB」という。)に承認され、記録されなければならない（個人情報保護法第 10 条及び第 12 条）。

(2) 当該原則が実質的に及ばない分野等について

特にない。

6. 公開の原則 (Openness Principle)

個人情報保護法には、公開の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

ア 個人データの取扱いに関する方針の策定に関する規定

上記5(1)のとおりに。

イ 個人データの存在と性質、主な利用目的、管理者の identity や所在地を容易に認識できる方法による提供に関する規定

個人データの存在及び性質、主な利用目的並びに管理者の身元及び所在地は、個人情報主体の同意に含まれなければならない、個人情報主体に事前に通知されなければならない（個人情報保護法第5条及び第6条）。

(2) 当該原則が実質的に及ばない分野等について

特になし。

7. 個人参加の原則 (Individual Participation Principle)

個人情報保護法には、個人参加の原則又はこれに対応する事業者・機関の義務に関する規定が一部存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

ア 自己に関する個人データの開示を求める権利を定める規定

保有者は、個人データの開示を請求する権利及び個人データの削除、訂正、完全性又は修正を請求する権利等を有する。コスタリカのすべての個人は、個人データへのアクセス、訂正、更新、及び削除の権利を行使し、司法又は行政機関を通じて効果的な法的救済を求めることができる。これらの権利は、データ輸入者の法域において適用される法律及び/又は慣行によって妨げられてはならない（個人情報保護法第7条及び第13条、並びに行政命令第12条、第13条、第15条乃至第26条）。

イ 自己に関する個人データの消去、訂正、完全化又は変更を求める権利を定める規定

上記アのとおりに。

ウ 権利行使ができない場合の理由の通知や異議申し立てを定める規定

特になし。

(2) 当該原則が実質的に及ばない分野等について

特にない。

8. 責任の原則 (Accountability Principle)

個人情報保護法には、責任の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

個人情報保護法第4章において、司法手続又は行政手続を通じて、裁判所又はPRODHABによる上記7原則の遵守を確保するための措置が規定されている。PRODHABは独立した基準を有し、違反の場合に制裁を課す権限を有する監督機関である。主に、経済的な罰金、データベースの停止、及び/又はデータの流通を防止するための差止命令ができる。PRODHABは、個人データの侵害に関する行政請求についての執行可能な裁定を発行し、また、行政機関は（職権により、又は影響を受けた当事者の要請に従い）個人データの削除、修正及び/又は更新を命令することができる（個人情報保護法第4章）。

司法上又は行政上のメカニズムを通じて、管轄権の保証を含め、効果的な法的救済を求める権利を定めている。さらに、PRODHABは法的強制力のある制裁を課すことができる（個人情報保護法第13条、第16(G)条、第24条及び第28条）。

(2) 当該原則が実質的に及ばない分野等について

特にない。

IV. 域内での保有・保管等の義務及びガバメントアクセス

1. データ・ローライゼーション規制 ①域内での保有・保管義務

個人情報・個人データを域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令⁷においては、現地法律事務所が把握している限り、存在しない。

2. データ・ローライゼーション規制 ②域外移転の制約による実質的な域内保持義務

個人情報・個人データの域外移転を制約することにより実質的に域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令⁸においては、現地法律事務所が把握している限り、存在しない。

⁷ 代表的か否かに関する判断は現地法律事務所が行っている。

⁸ 代表的か否かに関する判断は現地法律事務所が行っている。

3. ガバメントアクセス

ガバメントアクセスを根拠付ける法令として、1994年法律7425号、刑法、税法が挙げられるが、裁判所の命令又は決定のもと、刑事手続又は税務手続に基づく個人データへのアクセスを認めるものであり、我が国の制度と比較して、コスタリカへの個人データの越境移転に伴い当該個人データに係る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とは解されないことから、本報告書には記載しない。

V. データ保護機関の有無及び連絡先

PRODHAB (<http://www.prodhab.go.cr/Contactos/>)

電話：+506 2234 0189

電子メール：info@prodhab.go.cr

第5章 チュニジア（チュニジア共和国）

I. 個人情報の保護に関する法制度

1. 個人情報の保護に関する法制度の有無

個人情報の保護に関する包括的な法令として、[個人情報の保護に関する法律（法律第2004-63号）](#)（Law n° 2004-63 dated 27 July 2004 on the Protection of Personal Data）（以下「法」という。）が存在する。当該法令は2004年7月27日に施行されている。

2. 1. 記載の法令に関する基本的事項

(1) 適用対象者

公的部門と民間部門のいずれも対象とする。公的部門の対象として、公的機関、地方公共団体、公的行政機関が含まれており、地方自治体もその対象となる（法第53条）。ただし、法は、域内の個人の個人データのみをその保護対象としている。

(2) 個人情報の定義

「個人データ」とは、その起源や形態にかかわらず、直接的又は間接的に個人を識別できる、あるいはさまざまな記号やデータによって個人を識別できるようにした情報のうち、公的な生活に関する情報や法律でそのように規定されているものを除くすべてのものをいう（法第4条）。

「センシティブデータ」とは、直接的又は間接的に、人種や遺伝子の起源、宗教的信条、政治的、哲学的、労働組合への加盟、健康状態を明らかにする個人データをいう（法第14条）。

(3) 地理的適用範囲

法は、チュニジア国内の居住者の個人情報に限り適用される。ただし、チュニジア国内の住民の個人情報が他国へ移転した場合、法は域外適用される（法第50条、第51条、第52条、第90条）。

3. 留意点

チュニジアは、2019年に、個人データの自動化された処理に係る個人の保護に関する欧州評議会条約第108号の改正議定書を批准しており、これに適合するためのデータ保護法令の改正が行われる可能性がある。もっとも、当該改正の時期については明らかでない。

II. 当該外国の個人情報の保護に関する制度についての「一定の指標」となり得る情報の有無

チュニジアは、EU の十分性認定を取得しておらず、また具体的な取得等に係る手続はなされていない。

また、APEC の CBPR システムには加盟しておらず、また具体的な加盟等に係る手続はなされていない。

III. 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及び本人の権利に関する法令規定の有無

1. 収集制限の原則 (Collection Limitation Principle)

(1) 規定の存否と概要

I. に記載した法令には、収集制限の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 適法かつ公正な手段による取得その他収集の制限を定めた規定

個人データの処理には、関係者からの同意が必要とされる場所、同意取得に当たっては明示的な書面による同意が必要とされる (法第 27 条)。

また、法第 28 条は、「児童に関する個人データの処理は、その法定後見人の同意があり、かつ家庭裁判所裁判官の許可がなければ行うことができない。」と定める。本規程は要保護性の高い児童の個人データについては、より手続きを厳格とするものと考えられる。

イ 取得に際してのデータ主体への通知又はデータ主体からの同意取得を定めた規定

上記アのとおり、データ主体からの同意取得が必要とされ、その同意は明示的な書面によることが必要とされる (法第 27 条)。

例外的に、当該個人情報の処理が、①データ主体の利益のために行われる処理であり、データ主体に連絡することが不可能である場合、②データ主体からの同意の取得が不相応な努力を伴う場合、③個人データ取得の手続が法律若しくはデータ主体が当事者となる条約により定められている場合においては、データ主体からの同意が必要とされない (法第 29 条)。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

2. データ内容の原則 (Data Quality Principle)

(1) 規定の存否と概要

I. に記載した法令には、データ内容の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 利用目的に関連する限度での取扱いを定めた規定

個人データは、収集された目的以外の目的のために取り扱われてはならない（法第 12 条）。

イ 利用目的の達成に必要な範囲内における正確性の確保を定めた規定

「個人データは、収集された目的のために必要な範囲で公正に処理されなければならない。データ管理者はまた、これらのデータが正確かつ最新であることを保証しなければならない」（法第 11 条）とされており、個人データが正確かつ最新であることがデータ管理者によって保障される必要がある。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

3. 目的明確化の原則 (Purpose Specification Principle)

(1) 規定の存否と概要

I. に記載した法令には、目的明確化の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 取得時又はそれより前の個人データの利用目的の特定を定めた規定

個人データの収集は、適法、かつ、事前に定められた、明示的な目的のためにのみ行うことができる（法第 10 条）とされており、利用目的を明示することが必要とされる。

イ 特定された利用目的又は当該利用目的と矛盾しない目的の範囲内における利用を定めた規定

個人データは、収集された目的のために必要な範囲で公正に処理されなければならない（法第 11 条）とされており、特定された利用目的の範囲内で利用されることが

必要とされる。

ウ 利用目的の変更時における利用目的の特定を定めた規定

上記アと同じ。

(2) 当該原則が実質的に及ばない分野等について

個人データの取扱いは、個人情報主体が同意した場合、個人情報主体の重大な利益の保護のために取扱いが必要な場合、及び一定の科学的目的のために取扱いが必要とみなされる場合に限り、収集された目的とは異なる目的のためにのみ行うことができる（法第 12 条）、とされており、一定の科学的分野については収集された目的と異なる目的で利用が可能だと考えられる。

4. 利用制限の原則（Use Limitation Principle）

(1) 規定の存否と概要

I. に記載した法令には、利用制限の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア あらかじめ特定した利用目的の範囲を超えて開示すること又は利用可能な状態に置くことを制限する規定

個人データは、収集された目的のために必要な範囲で公正に処理されなければならない（法第 11 条）とされており、利用目的の範囲を超えた処理は制限されている。

イ あらかじめ特定した利用目的の範囲を超えてその他の利用を制限する規定

個人データの収集は、適法、かつ、事前に定められた、明示的な目的のためにのみ行うことができる（法第 10 条）とされており、利用目的の範囲を超えた利用は制限される。

(2) 当該原則が実質的に及ばない分野等について

個人データの取扱いは、個人情報主体が同意した場合、個人情報主体の重大な利益の保護のために取扱いが必要な場合、及び一定の科学的目的のために取扱いが必要とみなされる場合に限り、収集された目的とは異なる目的のためにのみ行うことができる（法第 12 条）、とされており、一定の科学的分野については収集された目的と異なる目的で利用が可能だと考えられる。

5. 安全保護の原則（Security Safeguards Principle）

I. に記載した法令には、安全保護の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

個人データを処理する者は、個人又は第三者を通じて、データのセキュリティを確保し、第三者が関係者の許可なしにデータを変更、又は参照することを防止するために必要なあらゆる予防措置を講じなければならない（法第 18 条）。

また、上記の予防措置は、下記のとおりでなければならない（法第 19 条）。

- ① 個人データの処理に使用される機器及び設備に権限のない者がアクセスできる状態又は場所に置かれないようにする。
- ② 承認されていないユーザーがデータキャリアを読み取り、コピー、変更、又は移動できないようにする。
- ③ 情報システムへの不正なデータの導入、及び記録されたデータの取得、消去又は削除を防止する。
- ④ 許可されていない者による情報処理システムの使用を防止する。
- ⑤ 情報システムにアクセスした者の身元、システムに入力されたデータ、入力時刻及びデータを入力した者が誰であるかをその後に確認できることを保証する。
- ⑥ データ通信又はその媒体の転送中にデータが読み取られ、コピーされ、変更され、消去され、又は削除されることを防止する。
- ⑦ 安全なバックアップ・コピーの構成によってデータを保護する。

上記に加え、データ管理者は、下請契約の枠組みの中である処理業務の全部又は一部を第三者に委託する場合、下請業者を周到に選択しなければならないと、当該下請業者は、法の規定を遵守しなければならないと、かつ管理者により許可された限度内でのみ行動しなければならないとされている。また、当該下請業者は、責任を有する任務を遂行するために必要かつ適切なすべての技術的手段を有していなければならないとされている（法第 20 条）。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

6. 公開の原則（Openness Principle）

(1) 規定の存否と概要

I. に記載した法令には、公開の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 個人データの取扱いに関する方針の策定に関する規定

個人データの取扱いには、個人データ保護に関する国家当局（National Authority for the Protection of Personal Data）（以下「INPDP」という。）の承認を必要としており、INPDP からの承認を得るためには、個人データの存在及び性質、主な利用目的並びに管理者の身元及び所在に関する情報を、INPDP に提供することが必要である（法第 8 条）。

イ 個人データの存在と性質、主な利用目的、管理者の identity や所在地を容易に認識できる方法による提供に関する規定

個人データの存在及び性質、主な利用目的並びに管理者の身元及び所在に関する情報 INPDP 及び個人データ主体に対して提供される必要がある（法第 7 条、第 8 条、第 31 条）。

(2) 当該原則が実質的に及ばない分野等について

下記の分野等においては、法第 8 条が適用されず、公開の原則が適用されない。

① 労働者の職務の状況に係る個人データの処理であって、当該処理が事業主により行われ、かつ、職務の遂行及び組織のために必要であると認められるもの（法第 16 条）

② 本人の健康状態の監視に必要な個人データの取扱い（法第 16 条）

③ 公的機関、地方公共団体、行政機関が防衛、訴追の枠組みの中で行う取扱い、又は現行の法律に従ってその任務を遂行するために必要な取扱い（法第 54 条）

7. 個人参加の原則（Individual Participation Principle）

I. に記載した法令には、個人参加の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

ア 自己に関する個人データの開示を求める権利を定める規定

アクセス権は、個人情報主体、その相続人、又はその後見人が本人に関連するすべての個人データについて照会する権利、及び法律により不正確である、不明瞭である、又は取扱いが禁止されていることが証明された場合に、これを訂正、完了、修正、更新、明確化、又は削除する権利として理解されるものとする（法第 32 条）とされており、自己に関する個人データを照会する権利について定められている。

イ 自己に関する個人データの消去、訂正、完全化又は変更を求める権利を定める規定

上記アと同様に、アクセス権は、個人情報主体、その相続人、又はその後見人が本人に関連するすべての個人データについて照会する権利、及び法律により不正確である、不明瞭である、又は取扱いが禁止されていることが証明された場合に、これを訂正、完了、修正、更新、明確化、又は削除する権利として理解されるものとする（法第 32 条）とされており、自己に関する個人データの消去、訂正、完全化又は変更を求める権利について定められている。

ウ 権利行使ができない場合の理由の通知や異議申し立てを定める規定

個人情報主体、その相続人又は後見人は、いつでも、有効、正当かつ重大な理由のために、本人に関する個人データの処理に異議を唱える権利を有する（法第 42 条）とされており、権利行使ができない場合の異議申し立てについて定められている。

(2) 当該原則が実質的に及ばない分野等について

下記の分野等においては、アクセス権の制限が許容される（法第 35 条）。

① 個人データの処理が科学的な目的のために行われ、かつそのデータがデータ主体のプライバシーに限定的な影響を与えるという条件付きで行われる場合

② アクセス権を制限する理由が、データ対象者自身又は第三者の保護である場合

8. 責任の原則 (Accountability Principle)

(1) 規定の存否と概要

I. に記載した法令には、責任の原則又はこれに対応する事業者・機関の義務に関する

る規定が一部存在する。具体的には、以下のとおりである。

INPDP から事前の許可を得ることなく、個人データを国外で処理又は国外に移転した場合、民事上及び刑事上の双方の制裁の対象となり得る（法第 86 条から第 105 条）。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

IV. 域内での保有・保管等の義務及びガバメントアクセス

1. データ・ローライゼーション規制 ①域内での保有・保管義務

個人情報・個人データを域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令⁹においては、現地法律事務所が把握している限り、存在しない。

2. データ・ローライゼーション規制 ②域外移転の制約による実質的な域内保持義務

個人情報・個人データの域外移転を制約することにより実質的に域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令¹⁰においては、現地法律事務所が把握している限り、存在しない。

ただし、法には個人データの域外移転規制自体は存在し（法第 25 条、第 52 条）、INPDP から事前の許可を得ることなく、個人データを国外で処理又は国外に移転した場合、民事上及び刑事上の双方の制裁の対象となり得る（法第 86 条から 105 条）。

3. ガバメントアクセス

I. に記載した法令は、公的機関、地方公共団体、公的行政機関が、公共の安全、国防又は刑事訴追のため、あるいは施行中の法律に従ってその任務を遂行するために当該処理が必要である場合には、個人データにアクセスすることが許可されている（法第 53 条）。

当該法令についての調査項目別の概要は以下のとおりである。

また、法律上の規定はないものの、裁判所の命令のもと、政府による個人データへのアクセスを認める制度が存在するが、これには裁判所からの命令が必要であり、我が国の制度と比較して、チュニジアへの個人データの越境移転に伴い当該個人データに係る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とは解されないことから、本報告書には記載しない。

(1) 法的根拠

⁹ 代表的か否かに関する判断は現地法律事務所が行っている。

¹⁰ 代表的か否かに関する判断は現地法律事務所が行っている。

ア 目的

公共の安全、国防又は刑事訴追のため（法第 53 条）

イ 実施主体

公的機関、地方公共団体、公的行政機関

ウ 取得される個人データの種類に関する限定の有無・概要

I. に記載した法令上、限定されていない。

エ 制限規定の有無・概要

公的機関、地方自治体、公的地方公共団体、公的行政機関は、個人データ主体、その法定代理人、相続人の書面による明示的な同意なしに、個人情報をも民間機関に伝達することを禁じられています（法第 57 条）。

オ 手続規定の有無・概要

I. に記載した法令上、規定されていない。

(2) 正当な目的の追求

I. に記載した法令上、規定されていない。ただし、チュニジア憲法第 24 条において、個人データの不可侵性について規定されている。

(3) 承認の要求

ア 事前承認及び事後承認、保護措置

I. に記載した法令上、規定されていない。

イ 暗号復号強制、保護措置

I. に記載した法令上、規定されていない。

(4) 取得された個人データの取扱いに対する制限

ア 保管期間の定めの有無・概要

行政機関は、特定の法律で定められた保存期間が終了した場合、又は個人情報を収集した目的が達成された場合、個人情報を破棄しなければならない。また、個人情報が法律で定められた活動にとって必要でなくなった場合にも破棄しなければならない（法第 61 条）。

イ データの取扱者に関する制限、保護措置

I. に記載した法令上、規定されていない。

ウ 安全管理措置に関する定めの有無・概要

I. に記載した法令上、規定されていない。

(5) 透明性

ア ガバメントアクセスの事実の通知義務の有無・概要

I. に記載した法令上、規定されていない。

イ ガバメントアクセスの実施状況の公表・公的機関に対する報告

行政機関は、行政報告書の作成義務がある（法第 61 条）。

ウ 監督機関による監督状況の公表

INPDP は、その活動に関する年次報告書を共和国大統領に提出する（法第 85 条）。

(6) 監督・調査・審査の仕組み

ア ガバメントアクセスの実施に対する監督・調査・審査の仕組みを規定する法令の有無・名称

I. に記載した法令上、規定されていない。

イ 監督機関の名称・権限・独立性・長の任命プロセスと身分保障

INPDP

ウ 調査形態

I. に記載した法令上、規定されていない。

エ 監督メカニズムの実効性を評価する仕組み・監督機関による公表の制度

I. に記載した法令上、規定されていない。

(7) 救済

ア 違法なガバメントアクセスに対する救済制度の有無・救済の内容・訴訟の結果を遵守する法的義務・救済手続の公表

救済を受ける権利は保証されている。(刑事訴訟法第 18 条)

イ 救済を提供する行政機関・裁判所

政府からも国会からも独立した、行政裁判所又は司法裁判所。

ウ 外国人の救済の可否

I. に記載した法令上、規定されていない。

エ ガバメントアクセスによって取得された情報に基づき訴追された者の権利

本人自ら、当該情報にアクセスすることが可能で、異議申し立てが可能である(刑事訴訟法第 193 条、第 194 条)。

V. データ保護機関の有無及び連絡先

National Authority of Personal Data Protection (<http://www.inpdp.nat.tn/>)

電話 : (+216) 71 799 853

電子メール : inpdp@inpdp.tn

第6章 パナマ共和国

I. 個人情報の保護に関する法制度

1. 個人情報の保護に関する法制度の有無

個人情報の保護に関する包括的な法令として、[2019年81号個人情報保護法](#)（Law No. 81 on Personal Data Protection 2019）（以下「Law 81」という。）が存在する。当該法令は国会により2019年3月29日に制定され、2021年3月29日に施行された。また、行政命令を通じた法に対する[規則285/2021](#)（Rules to the Law through Executive Order 285/2021）（以下「Rule 285」という。）も存在し、同規則は2021年5月8日に施行された。

2. 1. 記載の法令に関する基本的事項

(1) 適用対象者

Law 81 及び Rule 285 は、公的部門と民間部門のいずれも対象とする。

(2) 個人情報の定義

個人データとは、自然人を識別する又は識別可能である、自然人に関する一切の情報をいう（Law 81 4条）。なお、Law 81 は、域内に存在するデータベース及び域内に所在する管理者が取り扱っているデータベースに適用され、かかるデータベースに域外にあるデータ主体の個人データが含まれている場合には、当該域外にあるデータ主体の個人データも保護の対象となる。

(3) 地理的適用範囲

Law 81 及び Rule 285 は、国内で個人データを処理する者の他、国内の市場をターゲットにしてオンライン上で商業活動を行っている外国企業にも適用される（Law 81 5条及び Rule 285 2条）。

3. 留意点

Law 81 及び Rule 285 以外に、ヘルスケア分野、銀行分野、保険分野、クレジットカードに係る分野等、特定の分野に適用される法律が存在する。

II. 当該外国の個人情報の保護に関する制度についての「一定の指標」となり得る情報の有無

パナマは、EU の十分性認定を取得しておらず、また具体的な取得等に係る手続はなされていない。

また、APEC の CBPR システムに加盟しておらず、具体的な加盟等に係る手続もなされていない。

III. 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及び本人の権利に関する法令規定の有無

1. 収集制限の原則 (Collection Limitation Principle)

(1) 規定の存否と概要

I. に記載した法令には、収集制限の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 適法かつ公正な手段による取得その他収集の制限を定めた規定

個人データは、詐欺的、不公平及び違法な手段によらないで取得されなければならないという原則が定められている (Law 81 2 条)。

イ 取得に際してのデータ主体への通知又はデータ主体からの同意取得を定めた規定

個人データを取得する場合、原則としてデータ主体から同意を得ることが必要である (Law 81 4 条)。データ主体から同意を得るにあたっては、利用目的を通知しなければならない (Law 81 6 条)。

(2) 当該原則が実質的に及ばない分野等について

データ主体が当事者である契約を締結するために必要な場合や、データ主体が服する義務又は裁判所の命令を履行するのに必要な場合、その他法律で認められている個人データの取扱いが認められている場合には、例外的にデータ主体の同意を不要とする定めは I. に記載した法令に存在するものの (Law 81 11 条)、その他の当該原則が実質的に及ばない分野は検出されなかった。

2. データ内容の原則 (Data Quality Principle)

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 利用目的に関連する限度での取扱いを定めた規定

個人データは特定の目的にのみ取得され、目的と異なる理由に基づく処理をして

はならず、また目的に必要な期間を超えて保存してはならないという原則が定められている (Law 8 12 条)。

イ 利用目的の達成に必要な範囲内における正確性の確保を定めた規定

処理される個人データは、データ主体の現在の状況に対応する正確かつ更新されたものでなければならないという原則が定められている (Law 8 12 条)。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

3. 目的明確化の原則 (Purpose Specification Principle)

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 取得時又はそれより前の個人データの利用目的の特定を定めた規定

上記 1. (1) イ 参照。¹¹

イ 特定された利用目的又は当該利用目的と矛盾しない目的の範囲内における利用を定めた規定

上記 2. (1) ア 参照。

ウ 利用目的の変更時における利用目的の特定を定めた規定

変更時に利用目的を特定しなければならないことを明示的に定めた規定は検出されなかったものの、管理者は、原則として、データ主体から同意を得た目的以外で個人データを処理してはならないと定められていることに鑑みれば (Law 81 11 条)、変更した利用目的の下に個人データを利用する場合には、当該目的を特定の上、再度データ主体の同意を得ることが必要であると考えられる。

¹¹ 上記 1.(1)イで記載したとおり、個人データを取得する場合には、原則としてデータ主体から同意を得ることが必要であるところ (Law 81 4 条)、この同意を得るにあたっては、利用目的を通知しなければならないと定められている (Law 81 6 条)。したがって、個人データを取り扱う事業者は、個人データの利用目的を予め特定し、本人に通知した上で、同意の上個人データを取得しなければならない (すなわち取得前に個人データの利用目的を特定しなければならない) ものであり、参照条項が取得以前に個人データの利用目的の特定を定めた規定であると考えられる。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

4. 利用制限の原則 (Use Limitation Principle)

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア あらかじめ特定した利用目的の範囲を超えて開示すること又は利用可能な状態に置くことを制限する規定

上記 2. (1)ア参照。また、提供された個人データの承認されていないアクセスや利用を禁止し、秘密を保持すべき原則が定められている (Law 81 2 条)。

イ あらかじめ特定した利用目的の範囲を超えてその他の利用を制限する規定

上記 2. (1)ア参照。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

5. 安全保護の原則 (Security Safeguards Principle)

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定 (漏えい等のリスクに対する合理的な安全保護措置を義務付ける規定) が、以下のとおり存在する。

個人データの処理に責任のある者は、保管する個人データのセキュリティを確保するために必要な技術的及び組織的安全管理措置を講じなければならない (Law 81 2

条)。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

6. 公開の原則 (Openness Principle)

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が一部存在する。具体的には、以下のとおりである。

ア 個人データの取扱いに関する方針の策定に関する規定

データ保護機関は、管理者及び処理者に対して、Law 81 及び Rule 285 を遵守する自己統制のための仕組みを策定することを推進しており、このような自己統制の仕組みを導入した管理者又は処理者は、データ保護機関に対して承認申請をしなければならない (Rule 285 39 条)。

イ 個人データの存在と性質、主な利用目的、管理者の identity や所在地を容易に認識できる方法による提供に関する規定

利用目的を通知することは規定されているものの (Law 81 6 条)、その他の情報を提供すべきことを定めた規定は存在しない。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

7. 個人参加の原則 (Individual Participation Principle)

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が一部存在する。具体的には、以下のとおりである。

ア 自己に関する個人データの開示を求める権利を定める規定

データ主体は、管理者から、データベース中に保存又は取り扱われている個人データにアクセスする権利、並びに取得元及び利用目的の通知を要求する権利が認められている (Law 81 15 条)。

イ 自己に関する個人データの消去、訂正、完全化又は変更を求める権利を定める規定

データ主体は、管理者に対して、不正確な個人データ、目的に関連のない個人データ、不完全な個人データ、不正確な個人データ、更新されていない個人データ等について、修正を請求する権利及び削除を請求する権利を有する (Law 81 15 条)。

ウ 権利行使ができない場合の理由の通知や異議申し立てを定める規定

権利行使ができない場合の理由の通知やデータ保護機関等への異議申し立てを定める規定は検出されなかったものの、データ主体は、自らの個人データの取扱いについて、管理者及び処理者に異議を申し立てることができ、またいつでも取扱いの同意を撤回することができる (Law 81 15 条)。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

8. 責任の原則 (Accountability Principle)

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定 (上記 7 原則の遵守を確保するための措置に関する規定) が存在する。

具体的には、管理者は当該法令を遵守しなければならない、データ保護機関の監査及び監督に服しなければならない (Law 81 7 条)。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

IV. 域内での保有・保管等の義務及びガバメントアクセス

1. データ・ローカライゼーション規制 ①域内での保有・保管義務

個人情報・個人データを域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令においては、現地法律事務所が把握している限りは存在しない。

2. データ・ローカライゼーション規制 ②域外移転の制約による実質的な域内保持義務

個人情報・個人データの域外移転を制約することにより実質的に域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令においては、現地法律事務所が把握している限りは存在しない。

3. ガバメントアクセス

I. に記載した法令は、犯罪の予防、調査、勾留、起訴及び刑罰の執行のために権限のある行政機関が行う活動に対しては、適用対象外とされている (Law 81 3 条)。

もっとも、現地法律事務所が把握している限り、いかなる場合にガバメントアクセスが認められるかを具体的に明確にした法令は存在しない。

V. データ保護機関の有無及び連絡先

National Authority for Transparency and Access to Information (ANTAI)
(<https://www.antai.gob.pa/contactenos/>)

住所: Ave. del Prado, Building 713, Balboa, Ancon, Panama, Republic of Panama
電話: (507) 527-9270 to 74

第7章 ペルー共和国

I. 個人情報の保護に関する法制度

1. 個人情報の保護に関する法制度の有無

個人情報の保護に関する包括的な法令として、ペルー個人情報保護法（Peruvian Personal Data Protection Law（Law No. 29733）（以下「PDPL」という。）が存在する¹²。当該法令は立法府により制定され、2013年5月8日にかけて段階的に施行された。また、ペルー個人情報保護規則（Personal Data Protection Regulation, Supreme Decree No. 003-2013-JUS）（以下「PDPR」という。）も存在し、同規則も2013年5月8日に施行された¹³。

これに加えて、医療・健康分野、金融分野、刑事、公的分野では、別途個人情報の保護に関する法律が存在する。

2. 1. 記載の法令に関する基本的事項

(1) 適用対象者

PDPL 及び PDPR は、公的部門と民間部門のいずれも対象とする。

(2) 個人情報の定義

個人データとは、合理的な手段を用いて自然人を識別する又は識別可能にする情報（数字、アルファベット、図形、画像、音声情報及び個人の習慣その他の自然人に関する特性であって、合理的な手段を用いて、自然人を識別する又は識別可能にするものを含む。）をいう（PDPL 2(4)条及び PDPR 2(4)条）。ただし、PDPL は、域内の個人の個人データのみをその保護対象としている。

(3) 地理的適用範囲

PDPL 及び PDPR は、ペルー国内の管理者及び処理者の他、国内の管理者や処理者に代わって個人データを処理する国外の処理者、契約や国際法によってペルーの法律が適用される国外の管理者及び処理者、及び国内に存在する手段（“means”。これには、ペルー国内に所在する消費者を直接の対象とするクッキーを含み得ると解されている。）を使用する国外の管理者及び処理者にも適用される（PDPL 3条及び PDPR 5条）。

3. 留意点

現地法律事務所が把握している限り、特に存在しない。

¹² <https://spij.minjus.gob.pe/spij-ext-web/detallenorma/H1034642>

¹³ <https://spij.minjus.gob.pe/spij-ext-web/detallenorma/H1075450>

II. 当該外国の個人情報の保護に関する制度についての「一定の指標」となり得る情報の有無

ペルーは、EUの十分性認定を取得しておらず、また具体的な取得等に係る手続はなされていない。

また、APECのCBPRシステムに加盟しておらず、具体的な加盟等に係る手続もなされていない。

III. 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及び本人の権利に関する法令規定の有無

1. 収集制限の原則 (Collection Limitation Principle)

(1) 規定の存否と概要

I. に記載した法令には、収集制限の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 適法かつ公正な手段による取得その他収集の制限を定めた規定

個人データは法律に従って処理されなければならない、詐欺的、不公平及び違法な手段による個人データの取得は禁止されている (PDPL 4 条)。

イ 取得に際してのデータ主体への通知又はデータ主体からの同意取得を定めた規定

個人データを取得する前に、データ主体に対して、次に掲げる事項を提供しなければならない (PDPL 12(4) 条及び 18 条)。

- ① 個人データの管理者及び処理者の名称及び連絡先
- ② 個人データの処理目的
- ③ 開示を受ける第三者 (存在する場合には)
- ④ 個人データを保存する関連データベースの存在
- ⑤ 越境移転がある場合はその旨
- ⑥ 保存期間
- ⑦ 個人データの提供が強制されるか
- ⑧ 個人データの提供を拒否した場合の結果
- ⑨ データ主体が、個人データ、開示、修正、消去及び処理への異議申立に対して権利行使する方法

また、個人データを処理する場合には、法律で定める例外を除き、事前の、自由な意思による、明確な、情報提供を受けた上での同意 (インフォームドコンセント) を取得しなければならない (PDPL5 条、PDPR12 条)。

(2) 当該原則が実質的に及ばない分野等について

医療従事者が医療上の理由から健康状態に係る個人データを取得する場合や、規制当局が公衆衛生のためにこれを取得する場合、マネーロンダリングやテロリストへの資金提供を防ぐために財産的な情報を交換する場合、行政機関が法律に基づいて活動するにあたって個人データを取得及び移転する場合等、例外的にデータ主体の同意を不要とする定めはPDPLに存在するが（PDPL14条）、その他の当該原則が実質的に及ばない分野は検出されなかった。

2. データ内容の原則（Data Quality Principle）

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 利用目的に関連する限度での取扱いを定めた規定

管理者は、個人データの処理が、所得目的に関連し、取得目的に鑑みて過剰でないことを確認する義務を負う（PDPL 7条）。

イ 利用目的の達成に必要な範囲内における正確性の確保を定めた規定

処理される個人データは、真実かつ正確であり、可能な限り最新であり、かつ目的に照らして必要十分なものでなければならないとされている（PDPL 8条）。加えて、個人データは、目的に必要な限度かつ安全が確保された方法で保存されなければならないと定められている。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

3. 目的明確化の原則（Purpose Specification Principle）

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 取得時又はそれより前の個人データの利用目的の特定を定めた規定

上記 1. (1) イ参照

イ 特定された利用目的又は当該利用目的と矛盾しない目的の範囲内における利用を定めた規定

特定及び明示された正当な目的でのみ個人データを取得し、匿名化される場合を除いて、当該目的以外に個人データを処理してはならない (PDPL 6 条、PDPR 8 条)。

ウ 利用目的の変更時における利用目的の特定を定めた規定

I. に記載した法令に直接の規定はないものの、規制当局の基準によれば、変更された利用目的のために個人データを利用する場合、データ主体から同意を得ることが必要であるとされている。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

4. 利用制限の原則 (Use Limitation Principle)

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア あらかじめ特定した利用目的の範囲を超えて開示すること又は利用可能な状態に置くことを制限する規定

上記 1. (1) イ及び 2. (1) ア参照。

イ あらかじめ特定した利用目的の範囲を超えてその他の利用を制限する規定

上記 1. (1) イ及び 2. (1) ア参照。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

5. 安全保護の原則 (Security Safeguards Principle)

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定（漏えい等のリスクに対する合理的な安全保護措置を義務付ける規定）が、以下のとおり存在する。

管理者及び処理者は、個人データのセキュリティを確保するため及び法律に違反した取扱い（漏えい等を含む）を回避するために、必要となる技術的、組織的及び法的な安全管理措置を講じなければならない（PDPL 9 条及び PDPR 10 条）。かかる安全管理措置は、個人データの 카테고리や取扱いに応じた適切なものでなければならない（PDPL 9 条及び PDPR 10 条）。特に電子的記録に係る場合には、アクセス制御、定期的な検証、ログの管理、認証に関する安全管理措置等を講じなければならない（PDPR39 条から 46 条）。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

6. 公開の原則 (Openness Principle)

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 個人データの取扱いに関する方針の策定に関する規定

上記 1. (1)イ記載の情報について記載したプライバシーポリシーを策定し公開しなければならない（PDPR 13 条）。

イ 個人データの存在と性質、主な利用目的、管理者の identity や所在地を容易に認識できる方法による提供に関する規定

上記 1. (1)イ記載のとおり、データ主体に対して、個人データ処理の目的、個人データの管理者及び処理者の名称及び連絡先を提供しなければならない。また、データ主体は、管理者から、個人データやその取扱状況についての情報を取得することが認められている（PDPR 61 条）。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

7. 個人参加の原則（Individual Participation Principle）

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 自己に関する個人データの開示を求める権利を定める規定

データ主体は、管理者から、個人データやその取扱状況についての情報を取得することが認められている（PDPR 61 条）。

イ 自己に関する個人データの消去、訂正、完全化又は変更を求める権利を定める規定

データ主体は、管理者に対して、最新ではない情報や不正確な情報について、個人データのアップデート及び修正を請求する権利を有する（PDPR 64 条及び 65 条）。また、データ主体は、目的に鑑みて不必要又は関連性のない個人データや、取扱期限が切れた個人データ、同意が撤回された個人データや法令に違反して取り扱われた個人データに対して、消去を請求する権利を有する（PDPR 67 条）。

ウ 権利行使ができない場合の理由の通知や異議申し立てを定める規定

データ主体からの権利請求を拒絶する場合には、正当な理由によらなければならない。データ保護機関に対して異議申し立てができる旨を示さなければならない（PDPR 59 条）。データ主体は、権利請求が拒絶された場合、データ保護機関に対して、行政法上の異議申し立てをすることができる（PDPL 24 条）。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

8. 責任の原則 (Accountability Principle)

(1) 規定の存否と概要

データ保護機関は、2021年12月、責任の原則を導入する決定 (resolution) をした。現地法律事務所によれば、当該決定 (resolution) には法源としての効力が認められるとのことである。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

IV. 域内での保有・保管等の義務及びガバメントアクセス

1. データ・ローカライゼーション規制 ①域内での保有・保管義務

個人情報・個人データを域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令においては、現地法律事務所が把握している限りは存在しない。

2. データ・ローカライゼーション規制 ②域外移転の制約による実質的な域内保持義務

個人情報・個人データの域外移転を制約することにより実質的に域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令においては、現地法律事務所が把握している限りは存在しない。

3. ガバメントアクセス

ガバメントアクセスを根拠付ける法令として、政令 1182 号 (Legislative Decree No. 1182 (July 2015)) (以下「LD」という) があり、犯罪の捜査のために携帯電話その他電子機器の位置情報を取得することが認められているが、これには司法機関による要件充足が確認される必要があり (LD 5 条)、我が国の制度と比較して、個人データに係る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とは解されないことから、本報告書には記載しない。

V. データ保護機関の有無及び連絡先

National Authority for the Protection of Personal Information
(<https://www.gob.pe/anpd>)

住所: Scipión Llona, Miraflores, Lima, Perú.
メール: protegetusdatos@minjus.gob.pe
電話: +51(01)204-8020, extension number 1030

第8章 南アフリカ（南アフリカ共和国）

I. 個人情報の保護に関する法制度

1. 個人情報の保護に関する法制度の有無

個人情報の保護に関する包括的な法令として、[個人情報保護に関する法律](#)(the Protection of Personal Information Act 4 of 2013)（以下「POPIA」という。）が存在する。POPIAは2014年4月11日から2022年2月1日にかけて段階的に施行された。

また、[2000年情報アクセス促進法](#)(the Promotion of Access to Information Act, 2000)（以下「PAIA」という。）も、個人情報の保護に関する包括的な法令として存在する。PAIAはその大部分が2001年3月9日に施行されている。

2. 1. 記載の法令に関する基本的事項

(1) 適用対象者

公的部門と民間部門のいずれも対象とする。なお、域内で情報処理の対象となる場合は、POPIAが適用され、域外にあるデータ主体の個人データも保護の対象となる。

(2) 個人情報の定義

POPIAに基づく「個人情報」とは、特定可能な、生存している自然人及び特定可能な、既存の法人に関する情報であり、個人の以下の情報を含む。(POPIA第1条)

① 人種、性別妊娠の有無、婚姻状態、出身国、民族、又は社会的出身、肌の色、性的指向、年齢、身体的又は精神的状態、身体障害、宗教、良心、信念、文化、言語、及び出生、教育歴、医療歴、経済歴、犯罪歴、又は雇用歴

② 識別番号、記号、電子メールアドレス、物理アドレス、電話番号、位置情報、オンライン識別子、又はその他の特定の割り当て

③ 生体認証情報

④ 本人についての意見、見解、好み、又は他の個人の見解や意見

⑤ 暗黙的又は明示的に私的又は秘密の通信、又は元の通信の内容を明らかにする更なる通信

⑥ 当該個人に関する他の個人情報と共に表示されている場合、又は当該名称の開示自体が当該個人に関する情報を明らかにすることになる場合は、その名称

また、POPIAに基づく「特別個人情報」とは、以下に掲げる情報をいう。(POPIA第26条) ① 個人情報主体の宗教的又は哲学的信念、人種又は民族的出身、労働組合のメンバーシップ、政治的信条、健康又は性生活、又は生体情報

② 当該情報の以下に関連する範囲における個人情報主体の犯罪行為

(i) データ主体が犯した容疑のある犯罪

(ii) データ主体が犯した容疑のある犯罪に関する訴訟手続き又は処分

(3) 地理的適用範囲

POPIA は、下記に適用される。(POPIA 第 1 条、第 3 条(b)項)

- ① 南アフリカの居住者
- ② 南アフリカの居住者ではないものの、南アフリカ内で個人情報を処理するもの

ただし、POPIA は南アフリカ国外を目的地とし、南アフリカを経由のみする個人情報には適用されない。

3. 留意点

現地法律事務所が把握している限り、特に存在しない。

II. 当該外国の個人情報の保護に関する制度についての「一定の指標」となり得る情報の有無

南アフリカは、EU の十分性認定を取得しておらず、また具体的な取得等に係る手続はなされていない。

また、APEC の CBPR システムには加盟しておらず、また具体的な加盟等に係る手続はなされていない。

III. 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及び本人の権利に関する法令規定の有無

1. 収集制限の原則 (Collection Limitation Principle)

(1) 規定の存否と概要

I. に記載した法令には、収集制限の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 適法かつ公正な手段による取得その他収集の制限を定めた規定

個人情報の取扱い（収集を含む）はすべて適法でなければならない（POPIA 第 9 条）。

イ 取得に際してのデータ主体への通知又はデータ主体からの同意取得を定めた規定

個人情報の収集は個人情報主体から直接行われることが必要であり (POPIA 第 12 条第 1 項)、個人情報主体から個人情報を収集する場合には以下の内容の通知が必要である (POPIA 第 18 条)。

- ① 収集される情報及び情報が個人情報主体から収集されない場合はその情報源
- ② 責任者の氏名及び住所
- ③ 情報を収集する目的
- ④ 当該個人情報主体による情報の提供が任意であるか強制的であるか
- ⑤ 情報を提供しなかった場合の結果
- ⑥ 情報の収集を許可する又は要求する特定の法律
- ⑦ 該当する場合には、責任を負う当事者が当該情報を第三国又は国際機関に移転することを意図しているという事実及び当該第三国又は国際機関が当該情報に与える保護の水準
- ⑧以下の追加情報
 - 情報の受信者又は受信者のカテゴリー
 - 情報の性質又はカテゴリー
 - 収集された情報を修正し、アクセスする権利の存在
 - 個人情報の取扱いに対する異議申立権の存在
 - 情報規制機関に対し苦情を申し立てる権利
 - 情報規制機関の連絡先であって、情報が処理され、又は処理されない具体的な状況を考慮して、個人情報主体に関する処理が合理的であることを可能にするために必要なもの

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

2. データ内容の原則 (Data Quality Principle)

(1) 規定の存否と概要

I. に記載した法令には、データ内容の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 利用目的に関連する限度での取扱いを定めた規定

個人情報の記録は、次の場合を除き、情報が収集され又はその後処理された目的を達成するために必要な期間を超えて保持されてはならない (POPIA 第 14 条)。

- ① 法律により、記録の保存が要求されているか、許可されている
- ② 責任当事者 (単独で又は他者と共同して、個人情報の処理の目的及び手段を決定する公的又は私的な団体若しくはその他の者を指す。以下「責任当事者」という。) が、その機能又は活動に関連する合法的な目的のために記録を合理的に要求する
- ③ 当事者間の契約により、記録の保持が要求される

- ④ 個人情報主体又は個人情報主体が児童である場合は権限のある者が、記録の保持に同意した

イ 利用目的の達成に必要な範囲内における正確性の確保を定めた規定

責任当事者は、個人情報完全、正確であり、誤解を招くことがなく、必要に応じて更新されることを確実にするために合理的に実行可能な措置を講じなければならない、そうすることにより、責任当事者は、個人情報が収集される又はさらに処理される目的を考慮しなければならない（POPIA 第 16 条）。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

3. 目的明確化の原則（Purpose Specification Principle）

(1) 規定の存否と概要

I. に記載した法令には、目的明確化の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 取得時又はそれより前の個人データの利用目的の特定を定めた規定

個人情報の取得に当たっては、責任当事者の事業に関する特定の、明確に定義された合法的な目的のために個人情報を収集しなければならない（POPIA 第 13 条）。

イ 特定された利用目的又は当該利用目的と矛盾しない目的の範囲内における利用を定めた規定

存在しない。

ウ 利用目的の変更時における利用目的の特定を定めた規定

個人情報が異なる目的で処理される場合、又は当初の処理目的と矛盾する目的で処理される場合、当該処理は追加的な処理に該当し、追加的処理を行うため、その処理

が POPIA に基づき合法とされるには、その取扱いのための同意又はその他の合法的根拠を責任当事者が取得することが必要とされる（POPIA 第 14 条）。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

4. 利用制限の原則 (Use Limitation Principle)

(1) 規定の存否と概要

I. に記載した法令には、利用制限の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア あらかじめ特定した利用目的の範囲を超えて開示すること又は利用可能な状態に置くことを制限する規定

上記 1. (1) ア及び 3. (1) ア参照。

イ あらかじめ特定した利用目的の範囲を超えてその他の利用を制限する規定

個人情報の更なる取扱いは、個人情報が最初に収集された目的に従って、又はその目的に合致して行われなければならない（POPIA 第 15 条）。ただし、下記の場合にはあらかじめ特定した利用目的と両立する。

- ① データ主体の同意がある
- ② 情報が公的記録に存在する又はデータ主体によって意図的に公表された
- ③ 公的機関による法の維持に対する侵害を避けるため、法により課される義務を遵守するため、又は国家安全保障の利益のために、更なる取扱いが必要である
- ④ 公衆衛生若しくは安全又は個人情報主体若しくはその他の者の生命若しくは健康に対する脅威を防止し又は軽減するために、追加的な取扱いが必要である

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

5. 安全保護の原則 (Security Safeguards Principle)

(1) 規定の存否と概要

I. に記載した法令には、安全保護の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

責任を負う当事者は、個人情報喪失、損害又は不正な破壊及び個人情報への不法なアクセス又は個人情報の不正な処理を防止するために、適切かつ合理的な技術的及び組織的措置を用いて、自らが保有し又は自らの管理下にある個人情報の完全性を確保しなければならない (POPIA 第 19 条第 1 項)。

また、上記の義務を履行するため、責任当事者は、以下の合理的な措置を講じなければならない (POPIA 第 19 条第 2 項)。

- ① 保有又は管理する個人情報について、合理的に予見可能なすべての内部及び外部リスクを特定する
- ② 特定された危険に対する適当な安全措置を確立し及び維持する
- ③ 安全措置が効果的に実施されていることを定期的に検証する
- ④ 過去に実施された安全措置における新たな危険又は欠陥に対応し、安全措置が継続的に更新されることを確保する

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

6. 公開の原則 (Openness Principle)

(1) 規定の存否と概要

I. に記載した法令には、公開の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 個人データの取扱いに関する方針の策定に関する規定

POPIA 第 4 条では、責任者による又は責任者のための個人情報の合法的な取扱いのための以下の条件を規定している。

① 「説明責任」

責任当事者は、POPIA に基づくすべての条件の遵守を保証しなければならず、当該条件の履行に責任を負う（POPIA 第 8 条）。当該責任には、第三者又はサービスプロバイダーも POPIA の規定を遵守することを確保しなければならないことが含まれる（POPIA 第 21 条）。

② 「オープン性」

責任当事者はデータ主体との間の透明性を確保することを求められる（POPIA 第 17 条、第 18 条）。

③ 「セキュリティセーフガード」

責任当事者は、個人情報の滅失、毀損又は不正な破壊及び個人情報への違法なアクセス又は個人情報の違法な処理を防止するために、自己が保有し、又は自己の管理下にある個人情報の完全性を、適切かつ合理的な技術的及び組織的措置により確保しなければならない（POPIA 第 19 条）。

④ 「データ主体の参加」

データ主体は、十分な身元証明を提供した上で、責任当事者に対し、当該特定のデータ主体に関する個人情報を責任当事者が保有しているか否かについて無償で確認するよう要求する権利を有する（POPIA 第 23 条第 1 項(a)）。データ主体はその後、合理的な期間内に、所定の料金（もしあれば）で、情報にアクセスした第三者についての情報を含む個人情報の説明を要求することができる（POPIA 第 23 条第 1 項 (b)）。

イ 個人データの存在と性質、主な利用目的、管理者の identity や所在地を容易に認識できる方法による提供に関する規定

上記 6. (1) ア①及び同④参照。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

7. 個人参加の原則 (Individual Participation Principle)

I. に記載した法令には、個人参加の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

ア 自己に関する個人データの開示を求める権利を定める規定

データ主体は、十分な身元証明を提供した上で、責任当事者に対し、当該特定のデータ主体に関する個人情報を責任当事者が保有しているか否かを無償で確認することを要請する権利を有する。データ主体は、当該情報にアクセスした第三者についての情報を含め、合理的な期間内に所定の料金で（該当する場合）当該個人情報の説明を要請することができる。さらに、当該情報は、合理的な方法により、一般に理解できる形式でデータ主体に提供されなければならない（POPIA 第 23 条）。

もっとも、①当該開示が第三者に関する個人情報の不当な開示を伴う場合、②第三者の営業秘密が記載されている場合、③第三者の秘密が記載されている場合又は④当該記録が法的に秘匿特権の対象となる文書を含んでいる場合には、責任当事者は記録へのアクセスを拒否することができる（POPIA 第 23 条 4 項(a)）。

イ 自己に関する個人データの消去、訂正、完全化又は変更を求める権利を定める規定

データ主体は、責任当事者に対して、保有する又は管理するデータ主体の個人情報の訂正、削除又は破棄を要求することができる（POPIA 第 24 条）。

ウ 権利行使ができない場合の理由の通知や異議申し立てを定める規定

データ主体は、自己への個人データの開示を拒否された場合、PAIA に基づき、当該理由の通知を受ける。（PAIA 第 56 条）

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

8. 責任の原則（Accountability Principle）

(3) 規定の存否と概要

I. に記載した法令には、責任の原則又はこれに対応する事業者・機関の義務に関する

る規定が存在する。具体的には、以下のとおりである。

上記 6. (1) ア①のとおり、責任当事者は、POPIA に基づくすべての条件の遵守の保証が必要となる。POPIA を遵守しない場合、①1000 万 ZAR を上限とする制裁金 (POPIA 第 109 条)、②データ主体及び規制当局が提起する民事訴訟 (POPIA 第 99 条)、③10 年以下の罰金若しくは禁錮 (若しくはその両方)、又は 12 カ月以下の罰金若しくは禁錮 (若しくはその両方) の責任を負う刑事制裁 (POPIA 第 107 条) の対象となる可能性がある。

(4) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

IV. 域内での保有・保管等の義務及びガバメントアクセス

1. データ・ローカライゼーション規制 ①域内での保有・保管義務

個人情報・個人データを域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令14においては、現地法律事務所が把握している限り、存在しない。

2. データ・ローカライゼーション規制 ②域外移転の制約による実質的な域内保持義務

個人情報・個人データの域外移転を制約することにより実質的に域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令15においては、現地法律事務所が把握している限り、存在しない。(ただし、POPIA には個人データの域外移転規制自体は存在する (POPIA 第 72 条))。

3. ガバメントアクセス

南アフリカには、ガバメントアクセスを根拠付ける法令として PAIA、2001 年金融情報センター法 (the Financial Intelligence Centre Act, 2001)、2004 年腐敗行為防止・対策法 (the Prevention and Combating of Corrupt Activities Act, 2004)、2011 年税務行政法 (the Tax Administration Act, 2011)、2002 年通信傍受及び通信関連情報提供法の規制 (Regulation of Interception of Communications and Provision of Communication Related Information Act, 2002)、1994 年国家戦略情報法 (The National Strategic Intelligence Act, 1994)、サイバー犯罪防止法 (Cybercrimes Act) (https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf) がある。これらは裁判所の命令又は決定のもと、個人データへのアクセスを認めるものであり、我が国の制度と比較して、南アフリカへの個人データの越境移転に伴い当該個人データに係る本人の権利利益に重大な影響を及ぼす可能性のあ

¹⁴ 代表的か否かに関する判断は現地法律事務所が行っている。

¹⁵ 代表的か否かに関する判断は現地法律事務所が行っている。

る制度とは解されないことから、本報告書には記載しない。

V. データ保護機関の有無及び連絡先

Information Regulator of South Africa
(<https://www.inforegulator.org.za/contact.html>)

電話：なし

電子メール：enquiries@inforegulator.org.za

第9章 モロッコ（モロッコ王国）

I. 個人情報の保護に関する法制度

1. 個人情報の保護に関する法制度の有無

個人情報の保護に関する包括的な法令として、[個人データの取扱いに関する個人の保護に関する法律](#)（法律第 09-08 号）（Law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data）（以下「法」という。）が存在する。法は 2009 年 2 月 18 日に施行された。

2. 1. 記載の法令に関する基本的事項

(1) 適用対象者

公的部門と民間部門のいずれも対象とする。なお、法は、あらゆる自然人又は法人に適用され、域内で情報処理の対象となる場合は、域外にあるデータ主体の個人データも保護の対象となる。

(2) 個人情報の定義

「個人データ」とは、その媒体/支援にかかわらず、特定された又は特定可能な自然人に関連するあらゆる種類の情報と定義され、特定された又は特定可能な個人に関連する音声及び画像が含まれる。また、個人は、特に識別番号又は身体的、生理的、遺伝的、心理的、経済的、文化的若しくは社会的アイデンティティの 1 つ若しくは複数の特定の要素を参照することにより、直接又は間接的に識別される場合に、識別可能とみなされる。（法第 1 条）

(3) 地理的適用範囲

法は、下記を行う自然人及び法人に適用される。（法第 2 条）

- ① 法的形態にかかわらず、モロッコ国内における個人データの加工活動
- ② モロッコ国内に在住していないものの、個人データを処理するためにモロッコにある自動又は手動の装置を使用

上記②の場合、情報管理者はモロッコでデータ管理者を代表するための代表者を指名する必要があり、個人情報保護国会委員会（the National Control Commission for the Protection of Personal Data）（以下「CNPD」という。）に対し、自身の代表者を報告する必要がある。

3. 留意点

現地法律事務所が把握している限り、特に存在しない。

II. 当該外国の個人情報の保護に関する制度についての「一定の指標」となり得る情

報の有無

モロッコは、EU の十分性認定を取得しておらず、また具体的な取得等に係る手続はなされていない。

また、APEC の CBPR システムには加盟しておらず、また具体的な加盟等に係る手続はなされていない。

III. 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及び本人の権利に関する法令規定の有無

1. 収集制限の原則 (Collection Limitation Principle)

(1) 規定の存否と概要

I. に記載した法令には、収集制限の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 適法かつ公正な手段による取得その他収集の制限を定めた規定

個人データの取扱いは下記の要件を充足する必要がある (法第 3 条)。

- ① 公正かつ合法的に処理されること
- ② 明確かつ合法的な特定の目的のために収集され、目的と矛盾するような方法でさらに処理されないこと
- ③ 収集された目的及びその目的に照らして、適切かつ過度でないこと
- ④ あらゆる合理的な措置を講じることにより、データが正確であり、必要に応じて更新されていること
- ⑤ 収集された目的及びその後処理される目的に関して、不正確又は不完全なものは消去又は修正されること

イ 取得に際してのデータ主体への通知又はデータ主体からの同意取得を定めた規定

原則、データ主体は、データの処理前に当該データの管理者又はその代理人により、明示的、正確かつ明確な方法で、以下について通知を受けなければならない (法第 5 条)。

- ① 管理者及び該当する場合にはその代理人の身元
- ② 想定される個人的なデータ処理の目的
- ③ 以下のような追加情報
 - ・受信者又は受信者の属性
 - ・質問への回答が強制か任意のいずれか及び回答がない場合に起こりうる結果
 - ・データ主体に関する個人データへのアクセス及び修正を行う権利の存在。ただし、当該データが収集される特殊な状況を考慮し、データ主体に関して当該個人データの公正な取扱いを確保するために当該情報が必要な場合に限る

④ CNDP への宣言書の受領又は CNDP が発行した認可の特性

データ主体から個人データが収集されていない場合、管理者又はその代理人は、データ主体が既に当該情報を受領している場合を除き、データを保存する前に、又はデータを第三者に開示することが予定されている場合は遅くともデータの最初の開示時に、少なくとも上記の①、②及び③に記載の情報を個人情報主体に提供しなければならない。

オープンネットワークにおける個人データの収集の場合、データ主体は、自らの個人データがセキュリティ保証なしにネットワーク上で流通する可能性があること、及び、当該個人データが権限のない第三者によって読み取られ、使用される可能性があることについて知らされなければならない。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

2. データ内容の原則 (Data Quality Principle)

(1) 規定の存否と概要

I. に記載した法令には、データ内容の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 利用目的に関連する限度での取扱いを定めた規定

上記 1. (1) ア参照。

イ 利用目的の達成に必要な範囲内における正確性の確保を定めた規定

上記 1. (1) ア参照。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

3. 目的明確化の原則 (Purpose Specification Principle)

(1) 規定の存否と概要

I. に記載した法令には、目的明確化の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 取得時又はそれより前の個人データの利用目的の特定を定めた規定

自己の個人データの収集のために直接連絡を受けた個人は、管理者又はその代理人（当該個人が既に連絡を受けている場合を除く）が、予定されている個人的なデータ処理の目的について、明確、正確かつ明確な方法で、処理前に連絡を受けなければならない（法第5条）。

イ 特定された利用目的又は当該利用目的と矛盾しない目的の範囲内における利用を定めた規定

個人データは、収集され、さらに処理される目的に照らして、適切で、関連性があり、過剰でないものでなければならない（法第5条）。

ウ 利用目的の変更時における利用目的の特定を定めた規定

存在しない。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

4. 利用制限の原則（Use Limitation Principle）

(1) 規定の存否と概要

I. に記載した法令には、利用制限の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア あらかじめ特定した利用目的の範囲を超えて開示すること又は利用可能な状態に置くことを制限する規定

個人データ処理のためのデータ主体は、譲渡人及び譲受人の職務に直接関連する目的を遂行する目的でのみ、かつデータ主体の事前の同意を条件として、第三者に連絡することができる（法第4条）。

ただし、以下の各号いずれかの場合にはデータ主体の同意は必要とされない。

- ① データ主体又は管理者が従うべき法的義務の遵守としてデータが処理される
- ② データ主体が当事者である契約の履行、又は情報主体の要求による契約前の措置の実行
- ③ データ主体の身体的又は法的能力が不十分な場合に、データ主体の重要な利益を保護するため
- ④ 公益のために、又は管理者若しくはデータの通信先である第三者に加えられた能力と公的な権限を行使して実施されるタスクの遂行
- ⑤ 公益のために、又は管理者若しくはデータの通信先である第三者に与えられた公的な権限を行使して実施されるタスクの遂行

イ あらかじめ特定した利用目的の範囲を超えてその他の利用を制限する規定
存在しない。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

5. 安全保護の原則 (Security Safeguards Principle)

(1) 規定の存否と概要

I. に記載した法令には、安全保護の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

EU データ保護法と同様の方法で、個人データは適切な技術的及び組織的措置を用いて保護されなければならない (法第 23 条)。

管理者は、特に情報処理がネットワークを介したデータの伝送を伴う場合、偶発的又は違法な破壊、偶発的な損失、改ざん、不正な開示、アクセスから個人データを保護するための適切な技術及び組織的措置を実施しなければならない。その他すべての違法な形態の処理から保護する必要がある。これらの措置は、技術水準及び当該措置の実施に関連するコストを考慮した上で、処理のリスク及び保護されるべきデータの性質に適したレベルのセキュリティを確保しなければならない。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

6. 公開の原則 (Openness Principle)

(1) 規定の存否と概要

I. に記載した法令には、公開の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 個人データの取扱いに関する方針の策定に関する規定

個人データは正確でなければならない。また、必要に応じて更新されなければならない (法第 3.1 条(d))。

イ 個人データの存在と性質、主な利用目的、管理者の identity や所在地を容易に認識できる方法による提供に関する規定

存在しない。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

7. 個人参加の原則 (Individual Participation Principle)

I. に記載した法令には、個人参加の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

(1) 規定の存否と概要

ア 自己に関する個人データの開示を求める権利を定める規定

データ主体は、自己の身元を証明することで、合理的な間隔で、遅滞なく、無償で、管理者から以下を取得する権利を有する（法第7条）。

- ① 当該データ主体に関する個人データが取扱われているか否かについての確認、並びに取扱われる目的、取扱われるデータの種別及び個人データが伝達される受領者又は受領者の種別に関する情報
- ② 処理中の個人データ及び当該個人データの出所に関する入手可能な情報についての理解しやすい形式での連絡
- ③ 当該データ主体に関する個人データの自動処理の背後にある論理/論理的根拠

イ 自己に関する個人データの消去、訂正、完全化又は変更を求める権利を定める規定

データ主体は、本人であることを証明すれば、特にデータが不完全かつ不正確である場合、法に準拠していない個人情報の処理の更新、修正、削除、遮断を管理者から取得する権利を有し、管理者に対し、当該個人の費用負担なく、10日間以内に必要な訂正を行うよう求めることができる（法第8条）。

ウ 権利行使ができない場合の理由の通知や異議申し立てを定める規定

データ主体が、上記7.(1)アに従い、自己に関する個人データの開示を求めた際に、管理者が要求に直ちに応じることができない場合、受領通知を申請者に交付し、日付と署名を付し、回答延期の理由を明らかにしなければならない、管理者は直ちにCNDPに照会して、要求に回答する期限を設定しなければならない（法第7条）。

また、データ主体が、上記7.(1)イに従い、自己に関する個人データの訂正等を求め、管理者から期間内に回答が拒否された場合、又は回答が得られなかった場合、データ主体はCNDPに修正要求を提出することができ、CNDPはそのメンバーの1人に、必要なすべての調査を実施し、必要な修正をできるだけ早く行うように指示する（法第7条）。

さらに、上記 7. (1)イに従って要求された個人情報の更新、修正、削除、遮断が不可能でない場合、当該データ主体は、その旨を個人情報が伝達された第三者に通知する権利を有する（法第 8 条）。

(2) 当該原則が実質的に及ばない分野等について

以下の場合には、当該原則が実質的に及ばない（法第 6 条）。

- (ア) 国家防衛、モロッコ国の内外安全保障、犯罪の防止又は抑止のために収集及び処理が必要な個人情報の場合
- (イ) データ主体に通知することが不可能であることが判明した場合
- (ウ) 法律で個人データの記録又は通信が明示的に規定されている場合
- (エ) 報道、芸術、文学の目的に限って行われる個人データの処理の場合

8. 責任の原則 (Accountability Principle)

(1) 規定の存否と概要

I. に記載した法令には、責任の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

管理者が CNDP の決定に従うことを拒否した場合、個人の場合、6 カ月から 1 年の懲役及び/又は 1 万 MAD から 10 万 MAD までの罰金が科せられる（法第 63 条）。

また、法に違反する態様で個人データを処理した場合、違反の態様によって、3 カ月から 1 年の懲役及び/又は 1 万 MAD から 30 万 MAD までの罰金が科せられる（法第 52 条～第 61 条）。

上記の法令違反が法人によって行われた場合、罰金の上限は個人の倍額となる（法第 64 条）。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

IV. 域内での保有・保管等の義務及びガバメントアクセス

1. データ・ローカライゼーション規制 ①域内での保有・保管義務

個人情報・個人データを域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令¹⁶においては、現地法律事務所が把握している限り、存在しない。

2. データ・ローカライゼーション規制 ②域外移転の制約による実質的な域内保持義務

¹⁶ 代表的か否かに関する判断は現地法律事務所が行っている。

個人情報・個人データの域外移転を制約することにより実質的に域内で保有・保管することを義務付ける規定は、個人情報の保護に関する法令、サイバーセキュリティに関する法令、及びそれ以外の代表的な法令¹⁷においては、現地法律事務所が把握している限り、存在しない。(ただし、法には個人データの域外移転規制自体は存在する(法第43条))。

3. ガバメントアクセス

モロッコには、ガバメントアクセスを根拠付ける法令として国家防衛及び国家の内
外安全保障のために収集及び処理される個人データを対象とする、法2.4条、[モロッコ刑事訴訟法](#)(the Moroccan Criminal Procedure Code)がある。

これらは裁判所の命令又は決定のもと、個人データへのアクセスを認めるものであり、我が国の制度と比較して、モロッコへの個人データの越境移転に伴い当該個人データに係る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とは解されないことから、本報告書には記載しない。

V. データ保護機関の有無及び連絡先

Moroccan Data Protection Authority (<https://www.cndp.ma/fr/>)

電話：(212) 5 37 57 11 24

電子メール：contact@cndp.ma

¹⁷ 代表的か否かに関する判断は現地法律事務所が行っている。

第 10 章 モンゴル国

I. 個人情報の保護に関する法制度

1. 個人情報の保護に関する法制度の有無

個人情報の保護に関する包括的な法令として、[個人情報保護法](#) (Law on Personal Data Protection) (以下「LPDP」という。)が存在する。当該法令は 2021 年 12 月 17 日に立法府 (State Great Khural of Mongolia) により制定され、2022 年 5 月 1 日から施行されることが予定されている。

2. 1. 記載の法令に関する基本的事項

(1) 適用対象者

LPDP は、公的部門と民間部門のいずれも対象とする。

(2) 個人情報の定義

個人データとは、姓、名前、誕生日、生誕地、住所、所在地、市民登録番号、属性、教育、メンバーシップ、電子的な識別子その他の、直接又は間接問わず、自然人を識別する又は識別可能である情報をいう (LPDP4. 1. 11 条)。なお、現地法律事務所が把握している限り、域外に所在するモンゴル国民の個人情報も個人データとして保護されるものの、域外に所在するモンゴル国民ではないデータ主体の個人情報も個人データとして保護対象に含まれるかは明らかではない。

(3) 地理的適用範囲

LPDP 及びその規則はモンゴル国内にのみ適用され、国外に対しては適用がない。

3. 留意点

LPDP の施行は 2022 年 5 月 1 日からである。

II. 当該外国の個人情報の保護に関する制度についての「一定の指標」となり得る情報の有無

モンゴルは、EU の十分性認定を取得しておらず、また具体的な取得等に係る手続はなされていない。

また、APEC の CBPR システムに加盟しておらず、具体的な加盟等に係る手続もなされていない。

III. 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及び本人の権利に関する法令規定の有無

1. 収集制限の原則 (Collection Limitation Principle)

(1) 規定の存否と概要

I. に記載した法令には、収集制限の原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 適法かつ公正な手段による取得その他収集の制限を定めた規定

個人データの処理は、次に掲げる法的根拠のいずれかに基づかなければならない (LPDP 7.1 条)。

- ① データ主体の同意
- ② 法律に基づいた取得及び処理
- ③ 雇用中に管理者が法律に基づいて権利を行使又は義務を履行する場合
- ④ データ主体が当事者となっている契約の締結又は履行のために取得及び処理される場合
- ⑤ 個人を識別できないようにした上で、歴史的、科学的、芸術的及び文学的な作品の創作に使用する場合

法的根拠に基づかない個人データの取得、処理及び利用は禁じられている (LPDP 29.1 条)。

イ 取得に際してのデータ主体への通知又はデータ主体からの同意取得を定めた規定

個人データを取得、処理及び利用するにあたっては、データ主体に対して、法定の例外を除き、次に掲げる事項を提供した上で、書面又は電磁的記録による同意を取得しなければならない。 (LPDP 7 条及び 8.1 条)。

- ① 個人データの取得目的及び正当化理由
- ② 事業者・機関の名称及び連絡先
- ③ 処理されるデータのリスト
- ④ データ処理及び保存期間
- ⑤ データを公開するか否か
- ⑥ データを第三者に提供するか否か
- ⑦ 同意取消の条件

ただし、公衆の利益を保護するため又は取材の目的のために、個人データを取得又は処理する場合には、データ主体の同意は不要とされている (LPDP 12.1 条)。

(2) 当該原則が実質的に及ばない分野等について

競争法 4.1.6 条に定める、州又は地方基金との商品、業務及びサービスの確保に関

する参加者に関しての「特別関係人」を決定するに当たっては、データ主体の同意は不要であるとされている（LPDP 8.8条）。

2. データ内容の原則（Data Quality Principle）

（1）規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 利用目的に関連する限度での取扱いを定めた規定

データ主体から同意を得たときに特定されかつ示された利用目的と整合しない目的による、個人データの取得、処理及び利用は原則として禁止されている（LPDP 29.1項）。

イ 利用目的の達成に必要な範囲内における正確性の確保を定めた規定

個人データを取得、処理及び利用するための原則の一つとして、データの完全性を損なわないことが定められている（LPDP 5.1.6条）。

（2）当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

3. 目的明確化の原則（Purpose Specification Principle）

（3）規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 取得時又はそれより前の個人データの利用目的の特定を定めた規定

上記 1. (1)イ参照。

イ 特定された利用目的又は当該利用目的と矛盾しない目的の範囲内における利用を定めた規定

上記 2. (1) ア参照。

ウ 利用目的の変更時における利用目的の特定を定めた規定

変更された利用目的のために個人データを利用する場合、データ主体から同意を得ることが必要である（LPDP 8.10 条）。

(4) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

4. 利用制限の原則（Use Limitation Principle）

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア あらかじめ特定した利用目的の範囲を超えて開示すること又は利用可能な状態に置くことを制限する規定

上記 1. (1) イ及び 2. (1) ア参照。なお、別途、LPDP にしたがって情報を取得した者は、第三者に開示してはならないという原則も定められている（LPDP 29.3 条）。

イ あらかじめ特定した利用目的の範囲を超えてその他の利用を制限する規定

上記 1. (1) イ及び 2. (1) ア参照。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

5. 安全保護の原則（Security Safeguards Principle）

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定（漏えい等のリスクに対する合理的な安全保護措置を義務付ける規定）が、以下のとおり存在する。

管理者及び処理者は、データセキュリティを確保しなければならない（LPDP 20 条）。具体的には、管理者及び処理者は、データセキュリティのための内部規程、及び漏えい等が発生した場合に当局への報告及びデータ主体への通知のための規程を策定し遵守しなければならない。また、管理者及び処理者は、個人データの取得、処理及び利用のためのシステムを、機密性を保持しつつ完全に利用可能なものとするための一切の手段を講じなければならない。さらに、管理者及び処理者は、個人データの利用や消去等の制限に係る規程や指示を遵守しなければならない。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

6. 公開の原則（Openness Principle）

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が存在する。具体的には、以下のとおりである。

ア 個人データの取扱いに関する方針の策定に関する規定

管理者は個人データの取得、処理及び利用に関するポリシー及びルールを策定し遵守しなければならない（LPDP 18.2.1 条）。かかるポリシーの開示を義務付ける規定は存在しないものの、管理者は、データ主体の求めに応じて、取得した個人データ及びその利用についての情報を開示しなければならない（LPDP 18.2.8 条）。

イ 個人データの存在と性質、主な利用目的、管理者の identity や所在地を容易に認識できる方法による提供に関する規定

上記 1. (1) イ 参照。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

7. 個人参加の原則 (Individual Participation Principle)

(1) 規定の存否と概要

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定が一部存在する。具体的には、以下のとおりである。

ア 自己に関する個人データの開示を求める権利を定める規定

データ主体は、自らの個人データから取得、処理及び利用されたかどうかを知る権利を有する (LPDP 16. 1. 2 条)。また、データ主体は、所得された個人データ及びその利用についての情報の提供を請求することができる (LPDP 18. 2. 8 条)。

イ 自己に関する個人データの消去、訂正、完全化又は変更を求める権利を定める規定

データ主体は、不正確なデータについて、管理者に通知して個人データの修正及び追加を請求する権利を有する (LPDP 16. 1. 5 条)。また、データ主体は、法令に従った消去を請求する権利、並びに個人データの消去が法令で認められている場合及び取得が法令で禁じられている場合に、法令を遵守するよう要求する権利を有する (LPDP 16. 1. 6 条)。

ウ 権利行使ができない場合の理由の通知や異議申し立てを定める規定

理由の通知や異議申し立てを定める規定はない。

(2) 当該原則が実質的に及ばない分野等について

個別法の規定により当該原則が実質的に及ばない分野等は存在しない。

8. 責任の原則 (Accountability Principle)

I. に記載した法令には、当該原則又はこれに対応する事業者・機関の義務に関する規定 (上記 7 原則の遵守を確保するための措置に関する規定) が存在する。

具体的には、管理者は、個人データの収集、処理及び利用にあたっての規律を定めなければならないとされているうえ (LPDP 18. 2. 1 条)、個人データの収集、処理及び利用にあたって責任を有するとされている (LPDP 18. 2. 15 条)。

IV. 域内での保有・保管等の義務及びガバメントアクセス

1. データ・ローライゼーション規制 ①域内での保有・保管義務

個人情報・個人データを域内で保有・保管することを義務付ける規定は、現地法律事務所が把握している限り¹⁸、LPDP には存在しない。

もともと、以下に概要を述べるとおり、モンゴルで認可を受けた銀行、金融機関、信用機関においては、クレジット情報をモンゴル国外に移転することは禁じられている。

(1) 2011年クレジット情報に関する法律 (Law on Credit Information 2011)

モンゴルで認可を受けた銀行、金融機関、信用機関は、クレジット情報をモンゴル国外に移転してはならない(同法 9.3 条)。ただし、現地法律事務所が把握している限り、かかる域内での保有義務は、国内の金融機関等が取得した情報を対象とするに留まり、域外から移転された個人情報には適用されないものとされている。

2. データ・ローライゼーション規制 ②域外移転の制約による実質的な域内保持義務

個人情報・個人データの域外移転を制約することにより実質的に域内で保有・保管することを義務付ける規定は、条約で定められるような場合を除いて、現地法律事務所が把握している限り、存在しない。

3. ガバメントアクセス

ガバメントアクセスを根拠付ける法令が複数存在し、主なものとして LPDP、警察法 (Law on Police 2017)、覆面捜査法 (Law on Undercover Operations 1997) 及び刑事手続法 (Law on Criminal Proceeding 2017) がある¹⁹。当該法令についての調査項目別の概要は以下のとおりであり、政府の情報収集活動への協力義務を課す制度であって、本人の権利利益に重大な影響を及ぼす可能性のあるものは不見当である。

(1) 法的根拠

ア 目的

刑事司法及び国家の安全保障に限られる (LPDP 10.1 条、覆面捜査法 9.3 条、警

¹⁸ ただし、現地法律事務所の回答によれば、2021年12月17日付けで制定されたサイバーセキュリティ法は、2022年2月27日の時点で官報に記載されておらず、本調査にあたって同法の検討はできなかったとのことであった。

¹⁹ 例示された法令は現地法律事務所が挙げたものである。

察法 64.4 条及び刑事手続法 2.20 条)。

イ 実施主体

検察官及び警察官（刑事手続法 22.1 条、22.2 条及び 22.3 条）²⁰

ウ 取得される個人データの種類に関する限定の有無・概要

法令上限定されていない。

エ 制限規定の有無・概要

ネットワーク上の個人の特定や位置情報の取得等、一定の捜査行為を警察官が行う場合には、検察官の承認が必要となる（刑事手続法 22.1.3 条）²¹。

オ 手続規定の有無・概要

警察官が、検察官へ捜査のリクエストをするにあたっては、行為、目的、アクセスの対象及び場所を特定しなければならない（刑事手続法 22.3.1 条）²²。

(2) 正当な目的の追求

現地法律事務所が把握している限り、本項目の適用はないものの、一定の捜査行為について検察官へのリクエストをする場合には、目的を特定する必要がある（刑事手続法 22.3.1 条）²³。

(3) 承認の要求

ア 事前承認及び事後承認、保護措置

上記 3. (1) エ 参照。

²⁰ 現地法律事務所からの回答によれば、LPDP、警察法及び覆面捜査法で規定されているガバメントアクセスについても、刑事手続法 22.1 条から 22.3 条までが適用されるとのことである。

²¹ 現地法律事務所からの回答によれば、LPDP、警察法及び覆面捜査法で規定されているガバメントアクセスについても、刑事手続法 22.1.3 条が適用されるとのことである。

²² 現地法律事務所からの回答によれば、LPDP、警察法及び覆面捜査法で規定されているガバメントアクセスについても、刑事手続法 22.3.1 条が適用されるとのことである。

²³ 現地法律事務所からの回答によれば、LPDP、警察法及び覆面捜査法で規定されているガバメントアクセスについても、刑事手続法 22.3.1 条が適用されるとのことである。

イ 暗号復号強制、保護措置

該当する規定なし。

(4) 取得された個人データの取扱いに対する制限

ア 保管期間の定めの有無・概要

該当する規定なし。

イ データの取扱者に関する制限、保護措置

該当する規定なし。

ウ 安全管理措置に関する定めの有無・概要

該当する規定なし。

(5) 透明性

ア ガバメントアクセスの事実の通知義務の有無・概要

LPDPにおいて、管理者は、機微情報にあたる個人情報を利用するとき、同意を得た利用目的以外の目的で個人データを利用するとき、第三者に提供するとき等には、データ主体に通知しなければならないとされている（LPDP 21.1 条）。しかしながら、かかる通知義務は、現地法律事務所が理解している限り、ガバメントアクセスには原則として適用されない。

また、上述の LPDP の規定を除いて、データ主体に通知すべきことを要求する規定は存在しない。

イ ガバメントアクセスの実施状況の公表・公的機関に対する報告

該当する規定なし。

ウ 監督機関による監督状況の公表

該当する規定なし。

(6) 監督・調査・審査の仕組み

ア ガバメントアクセスの実施に対する監督・調査・審査の仕組みを規定する法令

の有無・名称

捜査手続は検察官の監督に服するものの、一般的な LPDP の遵守状況を監督する権限を持つ機関として、国家人権委員会 (National Human Rights Commission) がある (LPDP 24.1 条)。

イ 監督機関の名称・権限・独立性・長の任命プロセスと身分保障

国家人権委員会は、LPDP で保護されている人権や自由が侵害されている旨の苦情を受け付け、苦情に基づき又は自らの裁量により調査し、人権や自由が侵害されている又は侵害されるおそれがあると認めるときには、関係当局に要求や勧告を発することができる。

ウ 調査形態

上記 3. (6) イ 参照。

エ 監督メカニズムの実効性を評価する仕組み・監督機関による公表の制度

該当する規定なし。

(7) 救済

ア 違法なガバメントアクセスに対する救済制度の有無・救済の内容・訴訟の結果を遵守する法的義務・救済手続の公表

権利が侵害されたデータ主体は、刑事罰を求めること (刑法 13.12 条)、行政裁判所に対して違法な個人データの取得、処理及び利用を理由とする一般行政法上の訴状を提出すること、及びプライバシー侵害等を理由として不法行為に基づく損害賠償請求をすることができる。

イ 救済を提供する行政機関・裁判所

裁判所は、国家権力から独立している。

ウ 外国人の救済の可否

モンゴル国民と同様に救済される。

エ ガバメントアクセスによって取得された情報に基づき訴追された者の権利

該当する規定なし。

V. データ保護機関の有無及び連絡先

National Human Rights Commission (<https://en.nhrcm.gov.mn/>)

住所: Mongolia, Ulaanbaatar city, Chingeltei duureg, Independence square
Government building No.11, 5th floor

電話: +976 70000222

メール: info@nhrcm.gov.mn