## バミューダ諸島

### 1. サマリー

(1) 個人情報の保護に関する制度の有無

個人情報の保護に関する包括的な法令として Personal Information Protection Act 2016 が存在する。当該法令は 2016 年 6 月 27 日に成立し、2025 年 1 月 1 日に全面的に施行されている。

(2) 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

EU の十分性認定：なし
APEC の CBPR システム：なし

(3) 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

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については、以下のとおり。

① 収集制限の原則：上記法令に規定されている。
② データ内容の原則：上記法令に規定されている。
③ 目的明確化の原則：上記法令に規定されている。
④ 利用制限の原則：上記法令に規定されている。
⑤ 安全保護の原則：上記法令に規定されている。
⑥ 公開の原則：上記法令に規定されている。
⑦ 個人参加の原則：上記法令に規定されている。
⑧ 責任の原則：上記法令に規定されている。

(4) 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

■ 個人情報の域内保存義務に係る制度であって、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

－

■ 事業者に対し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

Companies Act 1981

会社に対し、会社法（Companies Act 1981）違反の調査のため、検察庁に個人情報を含む帳簿・文書の提出を義務付け。

## 2. 個人情報の保護に関する制度の有無

(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 Personal Information Protection Act 2016（以下「PIPA」という。）が存在する。PIPA は 2016 年 6 月 27 日に成立し、2025 年 1 月 1 日に全面的に施行されている。

(2) PIPA に関する基本的事項

ア. 適用対象者

PIPA は、バミューダにおいて個人情報を処理する全ての組織に適用される。組織とは、「個人情報を処理するあらゆる個人、事業者又は公的機関」と定義されており（PIPA2 条）、公的部門と民間部門双方を対象とする。なお、特定の公的機関を除外する規定はない。

イ. 保護対象の範囲

PIPA の保護の対象となる「個人情報」とは、「識別され又は識別可能な個人に関するあらゆる情報」と定義付けられている（PIPA2 条）。保護の対象となる「個人」とは、「自然人」と定義されており（PIPA2 条）、居住地又は国籍による区別はない。

ウ. 地理的適用範囲

PIPA は、域外適用について明示的な規定を設けていないが、その全部又は一部が自動化された手段による個人情報の処理、及び構造化されたファイリングシステムを形成し又は形成することが意図された個人情報の処理を行う組織に対して適用される（PIPA3 条）。

## 3. 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

バミューダ諸島は、EU の GDPR に基づく十分性認定を取得していない。

また、バミューダ諸島は、APEC の CBPR システムには加盟していない。

## 4. 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

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

PIPA には、収集制限の原則又はこれに対応する事業者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

組織は、適正かつ公正な手段で個人情報を取り扱わなければならない（PIPA8 条）。なお、「処理」とは「収集、取得、記録、保存等を含む個人情報に関するあらゆる業務の遂行」と定義されており（PIPA2 条）、取得や収集も含む。

イ. 取得に際しての本人への通知又は本人からの同意取得を定めた規定

組織は、本人が契約当事者となっている契約の履行のために必要な場合、法令によって要求されている場合、人の生命・健康・安全若しくは公益への危害を防止する緊急の必要性がある場合、公益上行うべき行為のために必要な場合、又は組織との現在・過去・未来の雇用関係の文脈で必要な場合等を除き、個人情報を処理する場合、本人の同意を取得する必要がある（PIPA6 条 1 項）。また、処理する個人情報がセンシティブ個人情報に該当する場合、原則として本人の同意が必要となる（PIPA7 条 3 項）。

組織は、利用目的、開示先を特定する情報、組織を特定する情報、プライバシーオフィサーの名前、利用制限のために組織が本人に提供する選択肢と手段等を含むプライバシーノーティスを本人に提供する必要があり（PIPA9 条 1 項）、組織は、個人情報の収集前若しくは収集時に（又はそれが不可能である場合には実務上可能な範囲で収集後速やかに）、プライバシーポリシーが本人に提供されるための合理的かつ実行可能な手段を講じなければならない（PIPA9 条 2 項）。

### (2) データ内容の原則（Data Quality Principle）

PIPA には、データ内容の原則又はこれに対応する事業者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

組織は、個人情報が、利用目的との関係で、適切で、関連性があり、かつ過剰でないことを確保しなければならない（PIPA11 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

組織は、個人情報が、利用目的との関係で、正確かつ最新の内容に保たれていることを確保しなければならない（PIPA12 条 1 項）。

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

PIPA には、目的明確化の原則又はこれに対応する事業者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

組織は、上記(1)イ.のとおり、利用目的を含むプライバシーノーティスを、個人情報の収集前若しくは収集時に（又はそれが不可能である場合には実務上可能な範囲で収集後速やかに）、本人に提供されるための合理的かつ実行可能な手段を講じなければならない（PIPA9 条 1 項、2 項）。

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

組織は、原則として、プライバシーノーティスに規定された特定の目的又はそれに関連する目的のためにのみ個人情報を処理することができる（PIPA10 条 1 項）。

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

利用目的の変更時における利用目的の特定を直截に定めた規定は存在しないが、当該変更について本人から同意を取り直す必要があると考えられる。

(4) 利用制限の原則（Use Limitation Principle）

PIPA には、利用制限の原則又はこれに対応する事業者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

組織は、原則として、プライバシーノーティスに規定された特定の目的又はそれに関連する目的のためにのみ個人情報を処理することができる（PIPA10 条 1 項）。但し、①本人が同意している場合、②本人の要求するサービス若しくは商品の提供に必要である場合、③法令若しくは裁判所の命令により要求される場合、④個人情報の不正利用の検出若しくは監視を目的とする場合、又は⑤個人の権利のための適切な保護措置が実施されることを条件として、科学的、統計的若しくは歴史的調査の目的で利用される場合には、例外的に、上記の利用目的制限は適用されない（PIPA10 条 2 項）。

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.と同じ。

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

PIPA には、安全保護の原則又はこれに対応する事業者の義務に関する規定（漏えい、滅失、毀損、不正アクセス、不正利用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）が存在する。具体的には、組織は、保有する個人情報を滅失、不正なアクセスその他の不正利用等のリスクから保護する適切な保護措置を講じなければならない（PIPA13 条）。

(6) 公開の原則（Openness Principle）

PIPA には、公開の原則又はこれに対応する事業者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. 個人情報の処理に関する方針の策定に関する規定

上記(1)イ.と同じ。

イ. 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)イ.と同じ。

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

PIPA には、個人参加の原則又はこれに対応する本人の権利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. 自己に関する個人情報の開示を求める権利を定める規定

本人は、原則として、組織の管理する自身の個人情報、個人情報の利用目的、及び個人情報の開示先の情報を得る権利を有する（PIPA17 条 1 項）。

イ. 自己に関する個人情報の消去、訂正、完全化又は変更を求める権利を定める規定

本人は、組織に対して、組織の管理する個人情報の訂正を要求する権利（PIPA19 条 1 項）、広告、マーケティング又は広報関係の目的での利用の停止を要求する権利（PIPA19 条 6 項）、本人又はその他の個人に対する重大な損害を生じさせる又はその可能性がある場合における利用の停止を要求する権利（PIPA19 条 8 項）、及び利用目的との関係で関連性が無くなった個人情報の消去又は破壊を要求する権利（PIPA19 条 10 項）を有する。

ウ. 権利行使ができない場合の理由の通知や異議申立てを定める規定

組織は、本人の権利行使の要求に対応しない場合は、本人に対して、書面で、拒否の理由及び異議申立てのために監督官庁に連絡する権利を通知しなければならない（PIPA20 条 13 項）。また、自己の個人情報に関して組織に対して権利行使の要求をした本人は、監督官庁に対して、組織の決定、作為又は不作為の審査を求めることができる（PIPA38 条 1 項）。

(8) 責任の原則（Accountability Principle）

PIPA には、責任の原則又はこれに対応する事業者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、組織は、PIPA 上規定された組織の義務及び個人の権利を実現するための適切な措置及び方針を採用しなければならず（PIPA5 条 1 項）、また、PIPA の遵守のための責任者であるプライバシーオフィサーを選任しなければならないとされている（PIPA5 条 4 項）。

## 5. 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

(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法令は、見当たらない。

(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法令は、見当たらない。

(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、Companies Act 1981 が存在する。

Companies Act 1981 は、276 条において、検察庁長官による大臣への申出により、大臣は、同法に基づく違反が行われた可能性があり、当該違反の実行に関する証拠が、会社の、又は会社が管理する帳簿・文書にあると思料する場合、当該帳簿・書類の全部又は一部を提示するよう文書で命ずることができるとしている。