

ガーンジー

1. サマリー

(1) 個人情報の保護に関する制度の有無

包括的な法令として、以下の法令が存在する。

- データ保護法 (Data Protection (Bailiwick of Guernsey) Law 2017)

URL

<https://www.guernseylegalresources.gg/CHttpHandler.ashx?documentid=80494>

- 施行状況：2018年5月25日施行
- 対象機関：公的部門及び民間部門
- 対象情報：特定された、又は特定可能な個人に関する情報

(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：2003年11月取得

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

EUの十分性認定取得国である場合、外国にある第三者に対する個人データの提供に伴うリスクについての本人の予測可能性は一定程度担保されると考えられるため、本項目に係る情報提供は必ずしも行う必要がない。

(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

Regulation of Investigatory Powers (Bailiwick of Guernsey) 2003

警察及び税関による国家安全保障や犯罪の防止又は検知等のため、個人情報を含む通信データの提出を義務付け。

2. 個人情報の保護に関する制度の有無

包括的な法令として、以下の法令が存在する。

■ データ保護法 (Data Protection (Bailiwick of Guernsey) Law 2017)

URL : <https://www.guernseylegalresources.gg/CHttpHandler.ashx?documentid=80494>

- 施行状況：2018年5月25日施行
- 対象機関：公的部門及び民間部門
- 対象情報：特定された、又は特定可能な個人に関する情報

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

ガーンジーは、2003年11月に欧州委員会の十分性認定を取得している。

また、ガーンジーは、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

ガーンジーは、欧州委員会の十分性認定を取得しているため、本項目の記載は省略する。

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。

データ保護法 (Data Protection (Bailiwick of Guernsey) Law 2017) 上、データ保護に関して十分なレベルの保護を提供している国 (EU 加盟国、英国及び欧州委員会の十分性認定を受けている国) 以外の国へ個人データを移転する場合には、一定の保護措置を講じた上で、データ主体がデータ主体の権利を行使し、有効な法的救済を受けるための仕組みが必要である。「一定の保護措置」には、当局が承認した拘束的企業準則

や標準契約条項¹等があり、少なくとも標準契約条項を締結して個人データの域外移転を行うことは、実務上一般的に不可能とは考え難いため、かかる規制は、実質的に域内で個人データを保有・保管することを義務付けるものではないと整理可能である。

(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、**Regulation of Investigatory Powers (Bailiwick of Guernsey) Law 2003**（以下「RIPL」という）が存在する。

RIPL は、通信傍受や通信データの取得・開示の権限及び制約について規定しており、RIPL により制約されている行為を行おうとする者は、「Her Majesty's Procurer」という政府の法機関の長の令状を得なければならないとされている。その例外として、通信データに関しては、警察の長及び税関の長が、一定の保護措置を講じた上で、第三者が保有する通信データへのアクセスを要求する権限を組織内の個人に付与できるとされている。権限を与えられた個人は、個人データを含む通信データの取得・開示要求通知を発することができ、通知を受けた者はこれに応じる義務を負うことになる。なお、権限を与えられた個人は、当該要求が国家安全保障や犯罪の防止・検知のために必要である等、RIPL の観点から必要なものであることを証明しなければならない。また、当局が入手したデータに暗号鍵（パスワード等のセキュリティ）が設定されている場合、当局は暗号鍵の開示を求める通知を発することができ、かかる通知に従わない場合には刑事罰の対象となり得る。

以 上

¹ ガーンジーは、欧州委員会の標準契約条項を利用することを承認している。