SO&SATO
INNOVATIVE LAWYERS

2019年7月12日

General Data Protection Regulation（EU一般データ保護規制）（GDPR）

-概観（パートI）

弁護士　佐藤　有紀

弁護士　小山　健太

フォーリンアソシエイト　Joerg Schmidt

昨年5月、GDPRの施行が開始された（EUデータ保護指令は置き換えられた）。それ以来、GDPRはEUのみならず、日本を含む各国において個人データ保護のための重要な判断基準と考えられている。EU内に所在する企業等の組織は、GDPRに日々精通してきているものの、EU域外の企業等組織では依然遵守状況についてはばらつきが見られる。GDPR施行から1年が経過した今、規制[1][2]の解釈を明確にしていきたい。

本稿では、GDPRにより保護される個人データとはどのようなものかということを踏まえて、GDPRがEU域外の組織にどの程度適用されるか概説する。第3項では、EU域内からEU域外への個人データの移管、特に日本への移管について、より詳しく見ていきたい。

1. 個人データとは?

GDPRは、個人データ（personal data）について、「識別され又は識別可能な自然人に関するあらゆる情報」と広く定義している。識別可能な自然人とは、データから直接的に、又は識別子(氏名、位置データ、オンライン識別子等)を参照することによって間接的に識別され得る自然人のことをいう。自然人がデータから識別できるかどうかを決定するためには、すべての合理的な手段（all reasonable means）を考慮しなければならない。特定の個人へ紐付けされ得ないデータは個人データではないため、GDPRの適用を受けない。[3]

個人データの例には以下のものがある。

- 氏名
- 自宅住所
- 氏名の表記を含むメールアドレス
- 位置データ
- IPアドレス

[1] 個人データの取扱いと関連する自然人の保護及び当該データの自由な移動に関する並びに指令 95/46/EC を廃止する2016年4月27日の欧州議会及び理事会規則(EU)2016/679

[2] 個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する1995年10月24日の欧州議会及び理事会の指令95/46/EC

[3] GDPR第4条第1項

2. GDPR はどのような行為に適用されるか?

GDPR は個人データの処理に適用される。処理の定義は非常に幅広く、個人データの収集、記録、編集、構造化、保存、修正、変更、検索、相談、使用、開示、配布、結合、制限、消去及び破棄が含まれる。[4]

処理の例としては、以下が挙げられる。

- 従業員管理・給与管理
- IP アドレスや MAC アドレスの保存
- 事業者による、個人の写真のウェブサイトへのアップロード

3. EU 域内に実体が無い事業者も GDPR を遵守すべき場合

GDPR の目的は、個人データの処理が EU との繋がりを有する場合に、高いレベルの保護を確保することである。したがって、GDPR は、当該個人データの処理が EU 域内に拠点を持たない組織による場合であっても、下記のいずれかの要件が満たされる場合には適用される。

(a) EU 域内に所在する拠点の活動として行われること。

(b) EU 域内に所在する個人に対する商品及びサービスの提供、又は EU 域内に所在する個人の行動のモニタリングに関連して行われること。

EU 域外に拠点を置く組織は、EU 域内における現状の配置・展開等が拠点とみなされるかどうか、もしみなされないとしても、個人データが拠点の活動に関連して処理されているかどうかを第一に検討すべきである。例えば、EU 域内に販売代理店がいるというだけでは「EU 域内に所在する拠点の活動」には該当しないが、以下で述べる要素を有する場合には（a）の要件を満たし、GDPR が適用されうる。

仮に（a）の要件に該当しない場合であっても、組織が EU 域内に所在する個人を対象としている場合、（b）の要件に該当するとして GDPR が適用されうる。

(1) EU 域内に所在する拠点の活動として行われること

GDPR は、EU 域内に所在する拠点の活動に関連する個人データの処理に適用される。当該処理が EU 域内では行われない場合であっても、GDPR の適用対象となる。

① EU 域内に所在する拠点

拠点とは、法律上の形式を問わず、安定的な仕組み（stable arrangements）を通じて、実効的かつ現実的な活動を行うものを意味する。したがって、EU 非加盟国の組織が EU 加盟国のいずれにも支店や子会社を有しないからといって、当該組織が EU 域内拠点を有しないとはいえない。従業員が一人、あるいは代理人が一人いる場合には、個々の人員が一定の永続性をもって行動する限り、安定的な仕組みをもっていると認

[4] GDPR 第 4 条(2)。

められる場合がある。

なお、EU 域内からホームページを閲覧できるという事実だけでは、EU 域外の組織が EU 域内に拠点を有すると判断される可能性は低いだろう。

② 域内拠点の活動としての処理

GDPR は、域内拠点自体がデータ処理を行うことを要請していない。しかしながら、GDPR が適用されるには、当該域内拠点の活動が、EU 域外組織のデータ処理活動と密接に関連していなければならない。そのような関連性が存在するかどうかは、事実と状況を考慮して、ケースバイケースで判断されることとなる。

個人データが EU 域外組織のデータ処理活動と密接に関連して処理される場合、GDPR は、当該データの主体である個人が EU 域内に所在するか否かにかかわらず適用される。GDPR は、「規則により与えられる保護は、その国籍又は居住地の如何を問わず、自然人の個人データの処理に関して自然人に適用されるべきである。」と明確に述べている。

例:

電子商取引プラットフォームを運営する日本企業が、EU 域内でマーケティング・キャンペーンを開始するために欧州事務所を設立した。データ処理業務は、日本所在の事務所が専任で行っている。
欧州事務所の活動は、プラットフォーム上で提供されるサービスをより収益性の高いものにすることを意図している。
このような場合、欧州事務所の活動は日本の電子商取引プラットフォームによって実行される個人データの処理と密接に関連している。よって、個人データの処理は、GDPR の適用を受ける。

(2) EU 域内の個人に対する物品又はサービスの提供及び域内の個人のモニタリング

急速な技術発展と国境を越えた個人情報の流れの増加を考慮して、EU 議会は EU 域内の個人を対象とする場合には GDPR が適用される旨を決定した。当該決定により、個人データの処理が以下のいずれかに関連する場合、GDPR が適用されることとなった。

(a) EU 域内の個人に対する商品又は役務の提供（支払が必要か否かを問わない。）

(b) EU 域内で行われる、個人の行動のモニタリング

① EU 域内の個人向け商品・サービスの提供

組織が EU 域内の個人に商品や役務を提供しているか判断要素としては、現地語の

使用、現地通貨の使用、欧州の顧客への言及、EU への送料の表示などが挙げられる。商品や役務を提供しているとされる場合、組織が EU 域内の個人の個人データを処理する際 GDPR が適用される。

例:

日本の事業者が、ウェブサイト上で、自社の Web 開発サービスについて申込みを受け付けている。そのウェブサイトは日本語、英語、スペイン語及びドイツ語で公開されている。報酬の支払いは、日本円、米ドル又はユーロで行うことができる。
当該サービスは EU 域内の顧客を対象としたサービスであり、ウェブサイトを運営する日本企業のデータ処理は GDPR の適用を受ける。

② EU 域内における個人の行動のモニタリング

個人データの処理は、当該データが EU 内の個人のモニタリングに関連する場合、GDPR の適用対象となる。典型的なケースは、クッキー及びトラッキングピクセルによるインターネット上のユーザの追跡、GPS データの収集及び行動広告である。GDPR が適用されるには、モニタリング対象者は EU 域内にいなければならない。EU 域内のモニタリングを監視することを意図しておらず、EU 内でのモニタリングが偶発的である場合、GDPR は適用されない。

例:

ヨーロッパの空港でストップオーバー中、日本人が日本のプレイストアでのみ提供されるアプリをダウンロードした。アプリは、各人の GPS データを追跡し、個人情報を収集する。
本アプリの開発会社は、EU 域内の個人データを収集する意図はないため、GDPR は適用されない。

4. 個人データの処理及び GDPR 違反に対する制裁

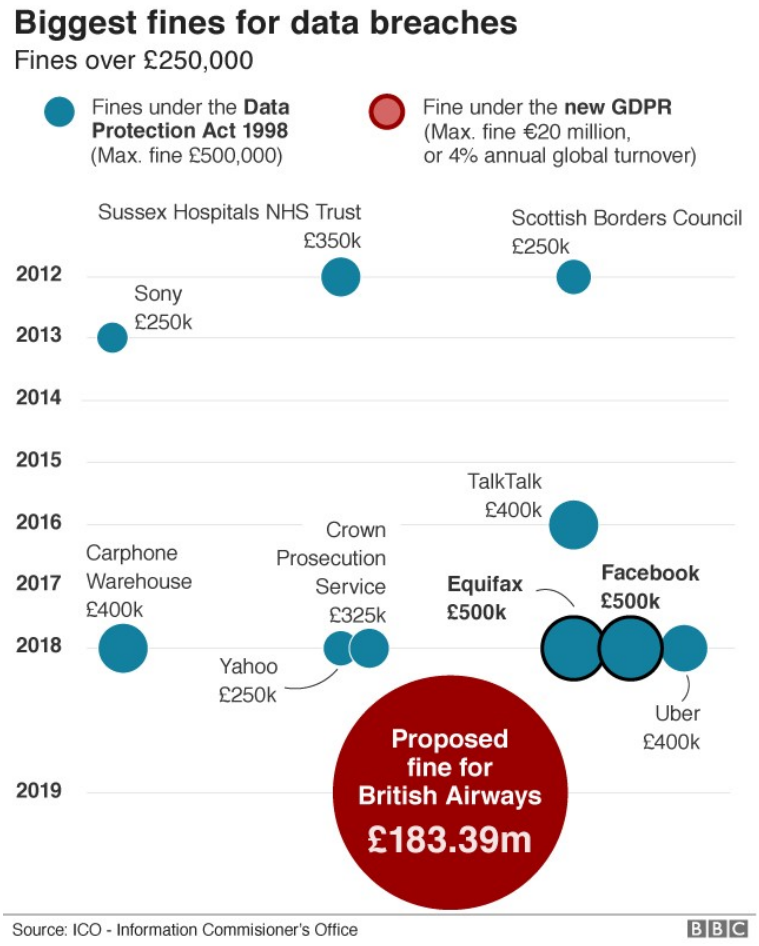
GDPR の下では、個人データの処理は適法でなければならない。適法な場合は、大まかに言って、以下のいずれかの場合に限られる。

- 個人が、所定の方法により、個人データの処理に自由意思に基づき同意した場合
- 当該個人が当事者である契約の履行のために処理が必要である場合
- 当該組織が法的義務を遵守するために処理が必要である場合
- その処理が個人若しくはその他の者の重大な利益（vital interests）を保護するために必要である場合

- その処理が公共の利益のために行われる業務の履行に必要である場合
- その処理が組織又は第三者による正当な利益の追求のために必要である場合

どのような場合にこれらに該当するかは次稿で検討することとする。

仮に個人データの処理が GDPR に違反していると判断されれば 20,000,000 ユーロ以下の制裁金、又は侵害者が事業体である場合には、前年度の全世界年間売上高の 4%以下の制裁金が課せられることがある。British Airways が GDPR に違反し、2017 年全世界年間売上高の 1.5%である約 250 億円の記録的な制裁金を課されたほか、ホテルグループの Marriott International に対して約 135 億円の制裁金が課された事例や、Google に対して約 62 億円の制裁金が課された事例などもあり、これに加え、レピュテーションリスクも過小評価されるべきではない。また、個人が違反者に対して損害賠償を請求したり、競争事業者が不正競争として苦情を申し立てたりすることもある。



図表：英国内における最大級の制裁金一覧（2012 年から 2019 年）[5]

[5] BBC（2019 年 7 月 8 日） 「British Airways faces record 183m fine for data breach」 ＜https://www.bbc.com/news/business-48905907＞ 2019 年 7 月 9 日アクセス

5. EU から日本や他の EU 域外諸国にいつ個人データを移すことができるか?

GDPR の下では、個人データは、組織が適切なセーフガードを実施している場合又は適用の免除が適用される場合にのみ、適切なレベルのデータ保護を提供する EU 域外諸国に移転することができる。

(1) EU から日本への個人データの移管はできるか?

欧州委員会は、2018 年、日本が個人情報について十分な水準の保護（いわゆる十分性認定、adequate level of protection）行っていると認定した。この認定は、日 EU 経済連携協定(EPA)及び戦略的パートナーシップ協定(SPA)の一環として行われ、2019 年 1 月 23 日に発効された。日本は現在、EU が十分性認定を行っている 13 か国の一つである。

以下は、欧州委員会が十分性認定を行っている国のリストである。米国については、Privacy Shield[6]が定めるルールに則って個人データを扱う場合に限り、EU 域内にある個人データを米国内に移管することができる。

アンドラ	アルゼンチン	カナダ	フェロー諸島
ガーンジー	イスラエル	マン島	日本
ジャージー代官管轄区	ニュージーランド	スイス	ウルグアイ
米国			

上記の国への個人データの転送には、当該国の法令に従う限り、関係する個人によるなんらの許可を必要とせず、また、なんらのセーフガードも不要である。この点で、データが自由に移転可能な EU 域内での個人データの転送に類似している。

我が国が欧州委員会から十分性認定がなされたことにより、（2）で述べるような煩雑な手続きがなされなくとも、EU 域内から日本に個人データを移管することができるようになった。疑義を避けるために付言すると、当然のことながら、日本企業は個人データの移転に関する条項以外の GDPR の条項の適用を免れるものではない。これに加えて、日本の個人情報の保護に関する法律と GDPR の齟齬を補完するためのルールである「個人情報の保護に関する法律に係る EU 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」が個人情報保護委員会から 2018 年 9 月に公表されており、EU 域内から日本に移転されたデータについては、当該ルールを遵守する必要がある。

(2) EU から上記以外の国への個人データの移管は可能か?

[6] EU に所在するデータ主体である自然人の救済手段の強化のため、自然人からの申立てへの 45 日以内の企業の対応義務などが設けられている。

欧州委員会による十分性認定がない場合、データは、適切なセーフガードが実施され、又はデータが移管された個人が法的救済を受けることができる場合に限り、EU以外の国に移管することができる。

適切なセーフガードには監督機関からの個別の承認を得る場合のほか、次のものが含まれる。

- EU 域内の個人データ保護機関により確認及び修正された、拘束力のある社内規則の実施
- 委員会が採択又は承認した標準データ保護条項（standard data protection rules）の使用
- 組織が、監督機関により承認された行動規範を、個人の権利を含む適切なセーフガードを適用するための拘束力のあり執行可能な誓約と共に使用すること。
- 組織が、監督機関により承認された個人データの移転に関する認証メカニズムを、個人の権利を含む適切なセーフガードを適用するための拘束力のあり執行可能な誓約と共に使用すること。

移転が適切なセーフガードに基づかない場合には、個人データは、適切なセーフガードがないことにより考えられるリスクについて個人が通知を受けた後に、当該個人が移転に明示的に同意した場合に限り、EU 域外諸国に移転することができる。

その他移転を行うことができる場合には、次の場合を含む。

- 個人と組織との間の契約の履行又は個人の請求により講じられる契約前の措置の実施のために移転が必要であること。
- 組織と第三者との間で、契約を締結し又は個人の利益のために締結された契約を履行するために譲渡が必要であること。
- 重要な公益上の理由により譲渡が必要であること。
- 移転が法的請求権の成立、行使又は防御のために必要であること
- 個人が同意を与えることができない場合で、個人又はその他の者の重大な利益（vital interests）を保護するために移転が必要であること。

6. まとめ

GDPR は、EU 域外の組織にも多くの影響を及ぼしており、違反には厳しい罰則が科されうること、GDPR の施行から約 1 年の間に GDPR 違反により多額の制裁金を課された事例が複数出てきていることからすると、日本企業としても、GDPR の適用を受けるか否かを改めて確認し、対応策を検討すべきであろう。

SO&SATO
INNOVATIVE LAWYERS

- 本稿の内容は、関係当局の確認を経たものではなく、法令上、合理的に考えられる議論を記載したものにすぎません。

- 本稿に記載の見解は、当職らの現状の見解に過ぎず、当職らの見解に変更が生じる可能性があります。

- 本稿は、Blog 用に纏めたものに過ぎず、また一般的な情報提供であり、具体的な法的助言ではありません。具体的な案件については、当該案件の個別状況に応じ、日本法または現地法弁護士の適切な助言を求めて頂く必要があります。

- 本稿の執筆者の連絡先は以下のとおりです。

弁護士　佐藤　有紀 (y.sato@innovationlaw.jp)

弁護士　小山　健太 (k.koyama@innovationlaw.jp)

フォーリンアソシエイト　Joerg Schmidt（j.schmidt@innovationlaw.jp）