押さえておきたいGDPRの基礎知識

弁護士
福山　龍

2018年5月25日に施行開始となった一般データ保護規則（GDPR）。「EUでの規制だから、うちの会社には関係ない」、「うちの会社にも影響がありそうだけど、どう影響するのか分からない」等、お考えの企業も少なくないのではないでしょうか。本稿では、GDPRの概要と基本的な注意点について、Q&A形式で解説します。

Q1. GDPRの主な用語がよく分からないのですが。

- 個人データ（personal data）: 個人を特定する、または個人の特定が可能なデータ。氏名やID番号等の典型的な個人情報のほか、IPアドレス等の位置データを含むあらゆる情報が含まれます。なお、ここで言う「個人」は、EU内に所在する個人を意味する一方で、それは国籍や居住場所を問わないため、例えば短期出張や出向でEU内に一時的に所在する日本人従業員の個人データも含まれます。
- データ主体（data subject）: 個人データを基に特定されたまたは特定可能な当該個人
- 管理者（controller）: 個人データの処理の目的と手段を決定する主体
- 処理者（processor）: 管理者からの委託で個人データを処理する主体
- 処理（processing）: 自動化された手段によるか否かにかかわらず、個人データもしくは個人データの集合に対して行われる一操作または一連の操作（例: 個人データの収集、保存、開示等）
- 移転（transfer）: EU外の第三国にデータを移転したり、第三国の第三者に対して個人データを閲覧可能にしたりする行為

Q2. GDPRとは一体何ですか？また、その適用範囲とは？

GDPRは、EU内に所在する各個人が自身の個人データを自由にコントロールする権利を保障する基本的人権の保護を強化する規則で、個人データを処理する事業者に対して多数の義務を課すものです。

GDPRは、1）EU内に「拠点」を有している、2）EU内居住者に商品やサービスを提供する、または3）EU内居住者の行動を「監視」する（クッキーやその他オンライン上の追跡機能等の使用を含む）管理者・処理者に対して適用されます。つまり、条件2）と3）により、GDPRはEU内に子会社や支店を持たない米国企業や日本企業にも適用可能性を有する法律なのです。

Q3. GDPRの適用対象となるとどうなりますか？また、どのような義務が生じますか？

企業がGDPRの適用対象となる場合、EU外に個人データを移転することは、移転先となる第三国で十分な保護レベルが存在すると欧州委員会が判断しない限り、原則違法です。但し、米国の企業においては、米国プライバシーシールド（個人データの保護に関する欧米間の枠組みで米国国務省への登録が必要）の条件を満たし、それに加入することにより、十分な保護レベルにあるとみなされてEU外への個人データ移転が可能となりますが、そうでなければ一定の保護措置を別途実施しなくてはなりません。また、主な義務の一例は次の通りです。

- 同意条項: 個人データを処理・移転するには、データ主体から自由意思に基づいた明確な「同意」を得る必要があります。従って、同意する旨のチェック欄が既にチェックしてあったり、同

増田・舟井・アイファート＆ミッチェル法律事務所
米国でビジネスを展開する日系企業およびその他国際企業を代理する法人向け総合法律事務所。日英バイリンガルの弁護士とスタッフが複数所属しており、米国進出、事業運営および事業拡大を含む事業ライフサイクルの各局面で、全米規模でのリーガル・サービスをワンストップで提供しています。

www.masudafunai.com

弁護士　福山　龍
業務分野は、コーポレート/ファイナンス/M&Aおよび商取引全般。早稲田大学法学部卒業（B.A.取得）。サンタクララ大学ロー・スクール卒業（J.D.取得）。

お問い合わせ:
弁護士　福山　龍
Email: rfukuyama@masudafunai.com
Tel: 312-245-7500

または、下記クライアント・サービス部門（電話番号は同上）までお気軽にご連絡下さい。

徳吉　史子
Email: ftokuyoshi@masudafunai.com

ローザ　里華
Email: rloza@masudafunai.com

意条項が契約書に埋もれていて他の条項と明白に区別されていなかったりする場合等は、有効な同意を得たとは言えません。また、同意の容易な撤回を可能にするシステムを導入する義務も生じます。

- 要求権への対応: GDPRは、データ主体が管理者に対して有する権利として、1) 個人データの消去や第三者への消去依頼を要求する権利、2) 自身の個人データの引渡しを要求する権利、3) 不正確な個人データの訂正を求める権利等を規定しており、管理者は、原則こうした要求に応える義務を負います。
- 通知義務: 管理者は、個人データの侵害が生じた場合、監督機関に通知する義務を負います。さらに侵害が個人の人権・自由を危険にさらす可能性がある場合には、監督機関のほか、データ主体にも通知しなくてはなりません。一方で、処理者においては、管理者に侵害について通知する義務を負います。
- 記録保持義務: 管理者は、個人データの処理操作の記録を保存する義務があります。当該義務が発生するのは、従業員数が250人以上の組織である管理者に限られますが、それを下回る規模の組織であっても、データ主体の人権・自由に高い危険を生じさせる可能性がある場合等には、当該義務が課される可能性があります。
- 代理人・DPO の選任義務: EU内に拠点を持たない一方で、EU内居住者への商品・サービスの提供において個人データを取り扱う管理者・処理者は、一定の場合において、GDPRの遵守に関して監督機関やデータ主体への対応窓口となる代理人（representative）をEU内で選任する必要があります。また、管理者・処理者が大規模且つ定期的な個人データの処理・移転を主な業務とする場合で、一定の条件に該当する場合には、組織内でのGDPRの遵守を監督するデータ保護最高責任者（Data Protection Officer: DPO）を選任する必要もあります。
- 個人データ処理に関する原則: GDPR第5条には、7つの基本原則が記してあります。この中で特筆すべき原則としては、1) 明示的且つ合法的な目的以外に個人データを収集しないこと、2) かかる目的を達成するために収集する個人データは最小限に留めること、3) 不正確なデータは遅延なく削除・訂正することが挙げられます。さらに、こうした基本原則への遵守を証明する責任も負います。

Q4. GDPR違反の制裁金は？

深刻なGDPR違反（同意取得における違反等）は、最高で2,000万ユーロ（もしくは企業であれば前年度の世界売上高の4%のいずれか高い方）となります。また、より軽度の違反（記録保持義務違反等）は、最高で1,000万ユーロ（もしくは企業であれば前年度の世界売上高の2%のいずれか高い方）となります。それ以外に、監督機関が違反企業を公表する等の可能性もあります。

Q5. GDPR施行により一般商業契約に変化は予想されますか？

GDPRを遵守するため、GDPR適用対象となる企業またはその恐れがあると自覚する企業は、取引先等に対しデータ保護補遺（Data Protection Addendum: DPA）への署名を既に要求し始めています。DPAにはGDPRへの遵守を義務付ける条項が含まれ、またヨーロッパの裁判所が管轄権を有することや、ヨーロッパの法律が適用されることへの同意条項が入ってる場合も多々あるため、DPAへの署名を要求された企業はDPAの必要性の有無を慎重に検討する必要があります。

本稿はあくまでも基本事項を概説するものであり、実際に各企業におけるGDPRの影響を判断するには、その事業様態を細かに検討する必要があります。各企業においては、事業運営上どのような個人データを取り扱っているか、またその中にEU内の個人データも含まれているか否か、GDPR施行開始を機に一度見直されてはいかがでしょうか。また、GDPRはEU加盟国自らが更に厳しい規則を導入する余地を残しているため、GDPRは「上限」ではなく「下限」に留まることを念頭に置き、EU加盟国の動向を注視していくことが重要です。