法務・労務・税務セミナー概要
（2022 年 7 月 7 日開催　於パリ）
講師：清水 怜雅弁護士 （DS AVOCATS Japan Desk）

2022年7月

ジェトロ・パリ事務所

テーマ： ＜EU 一般データ保護規則（GDPR）の留意点＞

① GDPR の適用範囲と制裁

GDPR は EEA（欧州経済領域）域内に在住する個人のデータ処理が適用範囲となり、GDPR の義務に違反した場合、企業は最大で全世界の総売上高の 4%または 2,000 万ユーロのいずれか高い方の制裁金が課される。制裁金は大企業のみならず、中小企業、自営業者にも課される。

② GDPR における個人データ保護のポイント

顧客リストのデータ変更、従業員の氏名・職務・連絡先などのリスト作成、メーリングのための顧客のメールアドレス収集など、個人データに対して行われるすべての操作が GDPR における個人データの「処理」とされる。個人データは明確かつ企業活動において正当な目的に適した範囲で収集され、その目的を達成するために処理されなければならない。例えば、商品送付のための顧客の住所収集、給与支払いのために必要な従業員情報の収集など、明確な目的を定めなければならないとされる。

個人データとは、識別された、または識別され得る自然人(データ主体)に関するすべての情報と定義される。具体例は以下のとおり。

（直接識別され得るデータ例 ）

氏名、証明写真、メールアドレス、個人のビデオ画像、身体的・遺伝的データ・バイオメトリックデータ、マイナンバー、社会保障番号

（間接的に識別され得るデータ例）

婚姻状況、社会的、地政学的データ、契約番号、カード番号、車のナンバー、消費に関する情報、オンライン識別子（IP アドレス、クッキー識別子等）

上記以外の以下の特別カテゴリーと呼ばれる、機密性の高い情報は、より高いレベルでのデータ保護が求められる。その結果、義務違反の場合の制裁もより厳しくなる。同カテゴリーのデータ処理が正当化されるのは、データ主体の同意、データ主体または個人の生命に係る利益の順守など、限られた場合となる。

（特別カテゴリー）

人種、政治的見解、哲学的または宗教的信念、労働組合の組合員であること、性的指向、健康データ、遺伝的データ・バイオメトリックデータ、 犯罪歴、社会・経済的状況

<u>データ管理者とデータ処理者</u>

データ管理者は、個人データの取り扱いの目的および方法を決定する者で、データ処理者は管理者に代わって個人データを処理する者である。データ管理者は、個人データの処理の適法性と GDPR 違反に対する責任を負う。また、グループ内の各社は自社の個人データファイルの作成と処理の責任を負う。利用するサービス会社、プラットフォームまたはシステムがGDPRに遵守して

いることを常に確認しなければならない。
データ処理者がデータ管理者に代わって処理を行う場合、データ管理者は適切な技術的かつ組織的措置を実施するため十分な保証を提供するデータ処理者を使わなければならない。また、データ処理者はデータ管理者と共同して責任を負うため、データ管理者と処理者が GDPR を遵守するように共同して作業を進めることが重要となる。

データ管理者またはデータ処理者は、下記の以下のいずれかに該当する場合にのみ、個人データ処理を適法に行うことができる。
- データ管理者が従うべき法的義務を順守するために処理が必要な場合
- データ主体がデータ処理に同意した場合、ただし事前に情報を与えたうえでの同意
- 契約履行または契約締結前の手続きを履践するために処理が必要な場合
- 公益のためにデータ処理が必要な場合
- データ管理者または第三者にとって追及される正当な利益のために処理が必要な場合
- データ主体または自然人の重大な利益を保護するために処理が必要な場合

個人データが侵害されたとみなされる状況は、事故によりまたは許可なく、①個人データが公開またはアクセスされた場合、②個人データが変更された場合、③個人データ破壊またはアクセス不可能となった場合の 3 パターンあるが、同時進行で起こることもある。個人データが侵害された場合、データ管理者は違反について、データ処理の記録を更新し、監督当局へ通知するとともに、データ主体へ通知を行う義務がある。

<u>個人データの処理における原則</u>
データ主体は、収集される個人データについて目的、移転先、権利および場合によっては侵害について通知されなければならず、場合により個人データの処理に同意しなければならない。また、目的に相容れない個人データの収集や、目的に相容れない方法での処理は認められない。目的に必要な範囲を超えて個人データを保管してはならないことから、一定期間の経過によりデータを削除するシステムを利用するなど、あらゆる合理的な手段を講じることが求められる。

<u>個人データ保護の新たな概念</u>
プライバシー・バイ・デザイン（Privacy by Design）
プライバシー保護に対して事後的な救済ではなく、新たなシステム・商品・サービスを構築する際に、その企画から保守段階までのすべてのライフサイクルで個人データ保護のための方策を技術面・運営面・設計面から作りこみ事前的な予防をする概念。

プライバシー・バイ・デフォルト （Privacy by Default）
データ処理システムの初期設定により、それぞれの目的に必要な個人データのみを収集し処理するために、適切な技術的及び組織的措置を講じる取り組みを行うこと。

③ GDPR への対策
GDPR に適合しているということは一時的な状態ではなく、新しい個人データ処理ごとに以下の一定事項を確認しなければならない。
- どのような個人データが収集されるか
- どのような処理が行われるか

- どのような目的のためか
- 誰に向けたものか
- 保管の期間は
- 移転先は
- どのように保護されるか

④ データマッピング

データマッピングとは、データを可視化し、業務プロセスの現状把握を行うことである。データの種類や収集目的、保存期間などを一覧表にまとめて、関係部署への確認や、関係者へのインタビューなどにより現状を把握する。EU 域外に移転する場合は、グループ間における取り決め、契約/規則などを締結する必要がある。

⑤ 個人データ保護の体制

データ保持者の権利の侵害が起こらないための保全、および侵害が起きた場合の修繕策を講じたことの証明が必要となる。コンプライアンスの対策として、プロセス・文書化、コントロールが重要となる。データ管理者、データ処理者のみならず、個々の従業員の意識を高めるためにも研修は重要である。

⑥ GDPR の法的措置

以下のような場合に個人データ保護責任者（Data Protection Officer,DPO）を選任する必要がある。

- 特別カテゴリーの個人データ並びに有罪判決・犯罪に関する個人データを大規模に処理する場合
- 組織の中心業務が、その性質、適用範囲、および/または目的によって、大規模にデータ主体の定期的かつ系統的な監視を必要とする処理をする場合

DPO の主な任務:

- 情報と助言の提供
- 適用される法令に則した個人データ保護方針の作成・更新およびその遵守の監視
- データ主体への事前通知
- 監督機関への協力
- リスクのある個人データ処理の監視
- 個人データ保護に関し社内での意識を高め、適正性の監査を監督する
- データ侵害があった場合の社内外への対応（監督機関及びデータ主体への通知）

DPO は GDPR および技術を含むその実務の専門知識を有し、他の任務や業務と DPO の任務が利益相反になってはならない。また、独立して任務を遂行でき、組織の経営最高レベルにのみ直接報告する。DPO は社内、社外（弁護士、コンサルなど）のどちらでもよく、ケースバイケースで選ぶ。

⑦ データ処理の記録

以下の条件に一つでも当てはまる場合、企業はすべての個人データ処理を記録し更新しなければならない。当てはまらない企業においても、社内での管理のために記録することを勧める。

- 従業員 250 人以上の場合

- データ処理により、データ主体の権利または自由が侵害されるリスクがある場合
- データ処理が恒常的に行われる場合
- 特別カテゴリーの個人データ処理を行う場合

記録内容は、データ管理者および DPO の氏名および連絡先、各データ処理の目的、法的根拠、詳細、データ主体およびデータの種類、データの受け取り先のカテゴリー、EEA 域外への移転および保護措置、保管期間、セキュリティ確保のための技術的および体制的措置、データ取り扱い開始日、最後に取り扱いを行った日、利用されたアプリケーション等。

⑧ データ主体の権利

データ主体は個人データの収集・処理の際に一定の情報を事前に提供されなければならない。サイトのプライバシー・ポリシーの中で明記すべきことである。

事前情報

- データ管理者の氏名
- データ処理の目的
- データの受け取り先
- データ収集および処理の法令または契約上の根拠
- データが収集されなかった場合の結果
- EEA 域外へのデータ移転および保障
- 間接的に情報収集される場合の収集源
- データ保管期間
- 個人データの自動処理の有無

データ主体は、データの情報権、アクセス権、訂正権、削除権、制限権、データポータビリティ権、自動化された個人の判断権を有する。

⑨ 個人データの移転

個人データの EEA 域外への移転は原則として違法である。移転先の国・地域が欧州委員会により「十分性」の認定を得ている場合、または適切な保護措置がとられている場合などにのみ例外的に適法となる。

日本、カナダ、スイス、イスラエルなど十分性認定国への移転は、データ主体への事前通知により個人データを適法に移転することができる。

中国、ペルー、モロッコなど十分性認定国以外への移転は、原則的に違法となり、本人への事前通知とは別に、データ主体の権利及び自由を保護するための適正な措置を取らなくてはならない。データ移転の煩雑さと頻度を考慮の上、標準契約条項（Standard Contractual Clauses, SCC）、または拘束的企業準則（Binding Corporate Rules, BCR）を作成することが望ましい。SCC は欧州委員会により決定された契約書のひな型であり、「管理者−管理者」および「管理者−処理者」の類型に従い企業ごとに締結する。BCR は企業グループ内でのデータ移転のみ適法化する措置である。監督機関による承認が必要なため、承認取得まで 18 カ月～2 年と期間と資料の英訳のための費用がかかる。

なお、2020 年 7 月より欧州・米国間のプライバシー・シールドは無効となり、米国へのデータ移転は十分性認定国以外の国への移転と同様の手続きが必要とされる。