M&P Legal Note 2018 No.5-1

GDPR（EU 一般データ保護規則）の概要

2018 年 6 月 4 日
松田綜合法律事務所
弁護士　加藤奈緒

第１　はじめに・GDPR の施行

2018 年 5 月 25 日、欧州連合（EU）における新しい個人データ保護の枠組みとして、一般データ保護規則（General Data Protection Regulation、以下「GDPR」といいます）が施行されました。

これまで EU での個人データの保護は、1995 年に制定された EU データ保護指令に基づき立法された各国のデータ保護法により個別に規律されていました。その後の情報通信技術の発展や、国際化に伴う情報収集・共有規模の拡大等を背景としたプライバシー保護強化の流れから、EU データ保護指令に代わり、欧州経済領域（EU 加盟国 28 カ国およびアイスランド、ノルウェー、リヒテンシュタイン。以下「EEA」といいます）に直接適用される統一的な規制として制定されたのが GDPR になります。従来よりも規制が強化され、また違反に対して厳しい行政罰が設けられているのが特徴です。

また、GDPR では、域内に拠点がない事業者についての域外適用の規定が設けられたため（後述）、EEA 域内に支店や子会社を持たない日本企業であっても、GDPR 対応が必要となる可能性があります。

本稿では、GDPR における規制の基本的な枠組みおよび事業者の義務の概要を中心に説明します。なお GDPR の条文解釈については、29 条作業部会という助言機関が策定するガイドラインが実務上の指針になってきますが、本稿時点では未だ公表されていないものも多く、今後も情報がアップデートされる可能性がある点にご留意下さい。

第２　基本的概念

GDPR は、端的には「個人データ」の「処理」と、EEA 域外への「移転」を規制する法律になります。それぞれの用語の定義は以下の通りです。

１　「個人データ」

「個人データ」とは、国籍や居住地を問わず、EEA 域内に所在する自然人を特定し得る個人データであり、例としては氏名、識別番号、位置データ、メールアドレス、クレジットカード情報、オンライン識別子（IP アドレス、クッキー）などが挙げられます。

ここでの「EEA 域内に所在する」とは、EEA 域内に居住する自然人に限られず、短期出張等で EEA 域内に所在する日本在住の日本人の情報や、日本企業から EU 内の関連企業に出向している従業員情報も含まれるとされています。

また、個人データのうち人種・民族的素性、政治的思想、宗教的信条、労働組合員資格に関する個人データ、健康関連データ、性生活もしくは性的指向に関するデータなど（いわゆるセンシティブデータ）および有罪判決・犯罪に係るデータについては、その処理について通常の個人データよりも厳格なルールが設けられています。

2　「処理」

GDPR における「処理」とは、自動的な手段であるか否かにかかわらず、個人データまたは個人データの集合に対して実施されるあらゆる単一または一連の作業とされています。例えば、以下の情報の取扱いはすべて個人データの処理に該当し得ます。

・クレジットカード情報の保存
・メールアドレスの収集
・顧客の連絡先情報の保存・変更
・従業員の業務評価の閲覧
・データ主体のオンライン識別子の削除
・顧客の購買履歴の閲覧
・従業員名簿の作成

3　「移転」

GDPR 上は「移転」の定義がありませんが、EEA 域外の第三国の主体に対して、個人データを閲覧可能にするためのあらゆる行為であると解釈されています。例えば、個人データを含んだ電子形式の文書を電子メールに添付して送ることや、EEA 域内のサーバにある個人データを EEA 域外から閲覧可能な状態に置くことも移転に該当すると考えられます。

4　管理者・処理者

個人データの処理を行う主体として、単独または共同で個人データの処理の目的と手段を決定する主体である「管理者」と、管理者を代理して個人データの処理を行う「処理者」のカテゴリでそれぞれ規制されています。

第３　GDPR の地理的範囲

GDPR は、事業者が EEA 域内に拠点を有する場合、「EEA 域内の管理者・処理者の拠点の活動に関連してなされる個人データの処理」について適用され、処理のなされる物理的な場所が EEA 域内か域外かを問わないとされています。したがって、EEA 域内に支店・子会社等の拠点を有する日本企業については、まずは当該拠点における GDPR への対応が必須となります。

また、EEA 域内に拠点を有しない場合であっても、(i)EEA 域内に所在するデータ主体に対して商品・サービスを提供する場合、(ii)EEA 域内で行われるデータ主体の行動をモニタリングする場合にも GDPR が適用されるとされています（域外適用）。域外適用のある事業者は、原則として個人データが処理されるデータ主体が居住する加盟国の一つに代理人を設置する義務が生じます。

上記(i)に関し、例えば日本国内のウェブサイトを通じて EEA 域内の顧客に対して商品やサービスを提供している事業者がこの要件を充足するかは、「事業者が EEA 域内に所在しているデータ主体に対して商品・サービスの提供を意図していることが明らかか否か」で判断するとされていますが、基準が必ずしも明確ではなく、個別の事案ごとの慎重な検討が必要になります。

第４　個人データの処理に関する規制

個人データの「処理」は、以下の①から⑥のいずれかに該当する場合のみ適法とされています。

① データ主体が特定の目的のために処理に同意した場合
② データ主体が当事者となっている契約の履行のために処理が必要な場合
③ 管理者の法的義務を遵守するために処理が必要な場合
④ データ主体、または他の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
⑤ 公共の利益または公的権限の行使のために行われる業務の遂行に処理が必要な場合
⑥ 管理者または第三者の追求する正当な利益のために処理が必要な場合

したがって、EEA 域内に所在する自然人から個人データを取得する事業者は、当該データの処理が上記のいずれかの適法化根拠を備えるようにするための措置を取る必要があります。実務上は、①②⑥のいずれかに依拠する場合が多いと思われますが、①の同意については任意性が要求され、かついつでも撤回が可能とされています。

また、事業者が個人データを収集・取得する際には、所定の事項（例として、管理者の身元および連絡先、処理の目的および法的根拠、その他の取得者および移転の詳細、データの保存期間、データ主体の権利の存在等）についてデータ主体に情報提供する義務が定められています。実務上は、当該事項を反映したプライバシーポリシーを策定し、データ主体がアクセスできる状況に置くという対応が取られています。

第５　個人データの移転に関する規制

EEA 域内で取得した個人データを EEA 域外へ「移転」させることは原則禁止されており、以下の要件に該当する場合のみ許容されています。

① 欧州委員会による十分性認定がなされている第三国への移転
② 移転によって生じ得るリスクについて情報が提供された上での、データ主体による明示的な合意
③ 標準契約条項（SCC）・標準データ保護条項（SDPC）を含む契約の締結による移転
④ 拘束的企業準則（BCR）による移転
⑤ 行動規範による移転
⑥ データ保護認証メカニズムによる移転
⑦ 特定の状況における例外（データ主体と管理者の契約の履行のために必要な場合等）

①の十分性認定による移転とは、欧州委員会が移転先のデータ保護レベルを評価した結果、特定の国・地域等が十分な保護のレベルを確保していると認定するという制度であり、十分性認定が得られた第三国への移転は許容されています。

日本は現在、個人情報保護委員会がこの十分性認定を得るためのガイドライン（移転を受けた個人データの取り扱いに関し遵守すべき規律を定めたガイドライン）を策定中であり、今秋にも認定を得る方向で協議を進めているとの報道がなされています。

③の標準契約条項（SCC）・標準データ保護条項（SDPC）とは、欧州委員会が定めたデータ移転のための契約書の雛形であり、移転元と移転先でこの雛型を使用して契約を締結することにより移転が許容されるとされています。

④–⑥の要件は監督官庁等の承認手続きを要するため、現状における EEA 域内から日本への個人データの移転についての実務的な対応としては、②③に依拠する場合が多いと思われます。

第６　GDPR の適用のある事業者の義務

上記のとおり、GDPR の適用のある事業者はその個人データの処理、域外への移転についての適法性要件を充たす必要があります。

また、以下をはじめとする多岐に亘る義務が発生するため、関連するシステムや社内体制の構築、規則の策定などの対応が必要となります。

■　記録保持義務

個人データの処理活動に関して、所定の事項を記録し保存する必要があります。なお、この記録保持義務に関しては従業員 250 名未満の事業者の適用除外規定が存在するものの、条文からは基準が明確ではなく、ガイドラインの公表が待たれています。

■　情報漏えい時の通知義務

個人データの侵害が発生した場合、管理者は不当な遅滞なく、可能であれば侵害に気づいてから 72 時間以内に監督当局に所定の事項を通知するこ

とが求められます。また、侵害がデータ主体の権利や自由に高いリスクを引き起こし得る場合には、不当な遅滞なくデータ主体に対して侵害を通知しなければならないとされています。

■　データ主体の権利の尊重

GPPR においては、アクセス権、訂正権、消去権、処理の制限権、データポータビリティの権利（管理者に提供した個人データを電子的形式で受け取り、他の管理者に移行できる権利）等のデータ主体の個人データに関する権利が定められており、データ主体からの権利行使があった場合、管理者はこれに対応する義務があります。

■　Data Protection Officer （DPO、データ保護責任者）の選任義務

管理者・処理者の中心的業務が、データ主体の大規模かつ定期的・体系的な監視や、センシティブデータの大規模な処理作業である場合、データ保護責任者の選任義務が発生します。

■　技術的・組織的なセキュリティ対策義務

■　データ保護影響評価の実施（体系的かつ広範囲なプロファイリングを実施する、センシティブデータを大規模に処理するなど一定の場合）

第７　制裁金

GDPR に違反した場合の制裁として、違反内容に応じて以下の２類型があり、非常に高額な上限が設定されています。

- 1000 万ユーロ、または企業の場合は前会計年度の全世界年間売上高の 2%のいずれか高い方を上限とする制裁金
- 2000 万ユーロ、または企業の場合は前会計年度の全世界年間売上高の 4%のいずれか高い方を上限とする制裁金

第８　最後に

これまで述べたとおり、GDPR は違反の場合の高額な制裁金のリスクがある一方で、事業者が対応すべき事項が多岐に亘り、かつ対応には時間・費用を要します。現時点で当局による違反の摘発例はまだ見られませんが、GDPR の適用があるものの現時点で対応が未了、あるいは検討中という企業については、できるだけ早期の戦略的な対策を講ずることが不可欠になります。

この記事に関するお問い合わせ、ご照会は以下の連絡先までご連絡ください

弁護士　加藤　奈緒
nao.kato@jmatsuda-law.com

松田綜合法律事務所
〒100-0004
東京都千代田区大手町二丁目６番１号
朝日生命大手町ビル７階
電話：03-3272-0101　FAX：03-3272-0102