M&P Legal Note 2019 No.1-1

GDPR（EU 一般データ保護規則）に関するアップデート①

2019 年 1 月 15 日
松田綜合法律事務所
弁護士　加藤奈緒

第１　はじめに

2018 年 5 月 25 日に一般データ保護規則(General Data Protection Regulation、以下「GDPR」といいます）が施行され半年あまりが経過しました。当事務所にも施行前後より GDPR 関連のご相談を多数いただいており、特にグローバルに事業展開する企業にとって検討が不可欠である一方で、未だ解釈や運用について不明確な点も多く、対応に悩まれる場面も多いのではないかと思料します。

本稿では、特にご質問の多い GDPR の地理的適用範囲について基本的な考え方を整理するとともに、実務上問題となるポイントについて解説いたします。合わせて、企業の皆様のご関心の高い日本の十分性認定に向けた手続の動向に関してもアップデートいたします。

第２　GDPR の地理的適用範囲

１　概要

GDPR が適用される地理的範囲は GDPR3 条 1 項及び 2 項に規定されており、具体的には以下の内容となっております。

① EEA 域内（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）の管理者または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。当該処理が EEA 域内または域外でなされるかを問わない（GDPR3 条 1 項）

② EEA 域内に拠点のない管理者または処理者による個人データの処理で、処理活動が以下の(a)または(b)に関連する場合（GDPR3 条 2 項）

(a)　EEA 域内に所在するデータ主体に対する商品・サービスの提供

(b)　EEA 域内で行われるデータ主体の行動の監視（モニタリング）

２　GDPR3 条 1 項

上記①の GDPR3 条 1 項の規定により、EEA 域内に支店・子会社等の拠点を有する日本企業にとっては、まず当該拠点が行っている個人データの処理活動について、GDPR に遵守した内容となっているかを確認することが不可欠となります。

加えて注意すべきなのは、この 3 条 1 項は、必ずしも「EEA 域内の拠点によって」行われる処理活動に限定されているわけではなく、「EEA 域内の拠点の活動に関連して（in the context of the activities of an establishment）」なされる個人データの処理に適用されるため、EEA 域内の拠点の活動に関連したものであれば、EEA 域外の企業が行う処理活動についても適用がありうるという点です。また、条文にあるとおり、当該処理活動が EEA 域内でなされるか域外でなされるかは問わないとされております。

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が、日本において個人データの処理を行っている場合であっても、当該処理が EEA 域内の拠点の活動に関連して行われる場合は、GDPR3 条 1 項の適用があると条文上は考えられます。例として、本社である日本企業が、EEA 域内の子会社への出向者の人事情報を、本社のデータベースにおいて管理している場合、たとえ処理の目的が本社における人事管理であったとしても、「EEA 域内の拠点の活動に関連して」なされる処理活動であると評価され、GDPR3 条 1 項の適用があるとされる可能性は否定できないように思われます。

「EEA 域内の拠点の活動に関連して」の解釈については、現在、欧州データ保護会議（EDPB・旧第 29 条作業部会）が GDPR3 条についてのガイドラインを策定中（本稿時点でパブリックコメント募集中）ですが、最終的には事例判断にならざるを得ないと思われ、対応については、処理する個人データの種類やリスクの度合い等に応じた具体的な判断が必要と考えます。

3　GDPR3 条 2 項(b)－行動の監視―

GDPR3 条 2 項はいわゆる域外適用と呼ばれる規定であり、EEA 域内に拠点を有しない事業者であっても、(a)EEA 域内のデータ主体に対する商品・サービスの提供、または(b)EEA 域内で行われるデータ主体の行動の監視に関連して個人データの処理を行っている場合は、当該処理につき GDPR の適用があるとされています。

この点、GDPR の施行当初は、(a)の規定により EEA 域内の個人を対象に E コマース事業を行っている企業等が適用対象になるとして大きく取り上げられておりました。他方で、(b)の「行動の監視」については相対的にあまり注目されていなかったような印象を受けます。

しかし、GDPR 前文によると、処理活動がデータ主体の行動の監視に関するものであるか否かを判断するためには、自然人がインターネット上で追跡されるかどうか、特に、データ主体に関連する判断をするため、またはデータ主体の個人的な嗜好、行動および傾向を分析または予測するために追跡されているかを確認すべきであるとされております（前文 24 項）。すなわち、「行動の監視」とは、インターネット上の追跡を想定した規定であることが読み取れます。

そして、GDPR における「個人データ」には、IP アドレスやクッキーといったオンライン識別子も該当するとされていることから、GDPR3 条 2 項(b)の「行動の監視」に該当する典型的な例として、クッキーを利用した行動ターゲティング広告が挙げられております。また、クッキーを利用したアクセス解析ツールにより、利用者のウェブサイトの閲覧履歴等を分析する行為についても、「行動の監視」に該当する可能性があると考えられています。

EEA 域内に拠点を有しておらず、また EEA 域内の個人に対して商品・サービスの提供を行っていない BtoB 事業中心の企業であっても、クッキーを利用した行動ターゲティング広告や企業サイトのアクセス解析を、特に地域の限定なく（EEA 域内も対象に含めて）行っている例は多いのではないかと思われます。これらの企業についても、GDPR への対応の要否について検討する必要があるということになります。

最近では、プライバシーポリシーとは別に、こうしたクッキーの利用についての詳細なポリシー（クッキーポリシー）を策定した上で、利用者によるウェブサイトへのアクセス時にポップアップ等で当該ポリシーを通知、同意を取得する企業も増えてきております。

第３　十分性認定に向けた手続

GDPR 上、EEA 域内から EEA 域外への個人データの「移転」は原則禁止されており、例外の一つとして、欧州委員会が十分なデータ保護のレベルを確保していると認定した国・地域等については移転が許容されております（いわゆる「十分性認定」）。

日本の十分性認定に向けた手続として、昨年９月に欧州委員会が日本の十分性認定手続の正式開始について閣議決定しており、合わせて個人情報保護委員会から「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」（十分性認定ガイドライン）が発表されました。日本が十分性認定を受け、これに基づき個人データがEEA域内から日本に移転された場合は、当該ガイドラインに従って個人データを取扱う必要があります（本ガイドラインの内容については、次回以降に解説させていただく予定です）。

昨年12月26日の個人情報保護委員会のプレスリリースによると、欧州委員会による日本の十分性認定の最終決定は本年１月中になる見込みとのことです。

このように、十分性認定については近い将来実現することが見込まれておりますが、誤解の多い点として、十分性認定はあくまで個人データの「移転」を許容する措置であって、例えばEEA域内のデータ主体から直接個人データを取得し、その「処理」についてGDPRが適用される例については、GDPRへの遵守が十分性認定によって不要となるわけではありません（この点、GDPRの条文上は必ずしも明確ではありませんが、個人データの「移転」は管理者または処理者間での移転を意味しており、EEA域内のデータ主体からの個人データの直接取得は「処理」に該当する一方、「移転」には該当しないと考えられます）。

したがって、今後日本の十分性認定がなされたからといって、GDPR対応が完全に不要になるわけではなく、許容されるのは「移転」の部分のみ、ということはご留意いただければと思います。

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