2019年6月21日
JIPDECセミナーレポート

ePrivacy規則案が与える日本企業の実務への影響

牛島総合法律事務所
弁護士　　影島　広泰　氏

関連する GDPR の規制

GDPR は施行されて 1 年が経つが、日本ではいまだ誤って理解されている部分もある。今回解説する ePrivacy 規則案は、GDPR の特別法にあたるため、まずは関係する GDPR について整理したい。

■GDPR の適用がある場合とは？

EU 域内で設立された拠点の活動に関連した個人データの処理に対して適用されるのは当然だが、重要なのは、EU 域外の日本法人の場合でも、以下のケースでは GDPR が域外適用されるという点である。

・EU 域内のデータ主体に対して商品やサービスを offer している場合

商品・サービスの「提供」と訳されている場合が多いが、正しくは「offer」しているかである。EU で使用されている言語や通貨による「注文」（order）が可能であったり、EU 域内の消費者・利用者に言及しているといった要素があると意図が明白と考えられ、offer していると評価され得る。一方で、例えば日本人を対象としたサービスがたまたま EU で利用されるようなケースに関しては GDPR の適用がないことを欧州委員会の Web サイトで明確に解説している。

・EU 域内のデータ主体に対してモニタリングをしている場合

商品やサービスを offer しているしていないに関わらず、EU 域内のデータ主体の行動の監視（典型的にはインターネット上のモニタリング＝トラッキング）は対象となる。これに関しては EDPB が地理的適用範囲に関するガイドライン案の中で、「監視という言葉はデータ収集およびその後の再利用という具体的目的をデータ管理者が念頭に置いている＝意図があることを示唆している」と述べている。行動をモニタリングするのではなく、Web サイトのアクセスログの保存のためだけのデータ収集は対象外となることになるのではないか。

なお、自社の活動が域外適用にあたると整理した場合は、現地に代理人を置く必要がある。

■個人データの定義と規制

GDPR の個人データの定義は、文言上は日本法と似ているが、例示の中に位置データ、オンライン識別子による識別が入っている点が異なる。e プライバシー規則案に大きく関連する部分についていえば、現状、多くの Cookie が個人データに該当するとみて運用されているのが大勢だと思われるが、識別され

うる情報が入っていない Cookie は個人データにあたらないとする意見もあり、見解が分かれるようである。

個人データ処理に関する諸原則（5条1項各号）の中で、日本企業が特に留意すべき点として、データ最小化の原則（目的に照らして最小限のデータのみ扱う）、保存制限の原則（不要データは即時削除する）が挙げられる。現在、このようないわゆる原則論を定めた条文に基づいて実際に課徴金が発生している。日本企業の事業部門では、「使うかもしれないので現時点では不要であるがデータを持っていたい」という要望が多く聞かれるが、これは GDPR では認められないということである。

■適法な処理となるための条件

GDPR の「同意」は非常に厳格で、声明または明らかに積極的な行為による明確な意思表示に基づくものに限定される。沈黙やあらかじめ入力されているチェックボックス、不作為は同意に該当しない。最近 Web サイトの Cookie に関するポップアップで「このサイトを閲覧し続けることで Cookie の取扱いに同意したものとみなします」と表示させるケースが見られるが、その Cookie が個人データに該当するということであれば、不作為という点で黒に近いグレーではないかと思われる。

1）従業員情報の取扱い

GDPR 前文において、「自由な選択肢がない同意は存在しない」とされており、その点で従業員情報の取り扱いに注意が必要となってくる。同意に関するガイドラインには、「雇用者と従業員の関係の性質上、従業員の同意ではありえないし、あるべきではない。」と明記されており、原則として同意に基づく従業員データの取扱いは禁止されている。従業員情報に関しては、契約履行や法的義務を法的根拠とする必要がある。

2）正当な利益（legitimate interests）による取扱い

legitimate interests は非常に重要な法的根拠となる。管理者にとって正当な利益がある場合には同意なく処理できるため、実務では多用されている。企業グループ内での顧客情報の共有やセキュリティ上の監視も、これにより同意なく可能となり得る。

■情報提供義務（13 条、14 条　直接・間接取得）

GDPR では、日本の個人情報保護法や JIS Q15001 よりさらに詳細に 12 個の情報提供義務がある。この情報提供義務と同意の取得を以て、GDPR の基本コンセプトである「Informed Consent」を形成している点で非常に重要となる。Informed Consent ができていることが、GDPR 対応の根幹部分の対応ができていることを意味するといえる。

実務的には、自社 Web サイトのプライバシーポリシーに 12 項目を記載すれば情報提供していると考えることができるのが通常であるが、個人がそれに容易に気づき、容易にアクセスできるよう考慮する必要がある。

ePrivacy 規則案

ePrivacy 規則案は GDPR の特別法となるため、個人データに関し ePrivacy 規則に特別の規定があれば

そちらが適用され、特に規定がない場合はGDPRが適用される。EDPBが出したGDPRと現行のePrivacy指令に関する意見では、Webトラフィックデータの処理に関してはePrivacy指令で規定されているためGDPRの適用は受けず、データ主体の権利に関してはGDPRのみが規定しているためGDPRが適用される。また、データブローカーがCookieを利用し他社から取得した個人データも含めてプロファイリングを行っている場合には、Cookieの保存、読み出しはePrivacy指令（に対応した国内法）に従い、その後の個人データの処理はGDPR6条による法的根拠が必要、としている。

■域外適用と規制対象

ePrivacy規則は、法人所在地に関係なく、EU域内のエンドユーザの電子通信データまたは個人データの処理が行われる場合に適用される。域外適用を受ける場合、現地代理人の選任が必要となる。

また、規制の対象としては、電子通信コンテンツ及び電子通信メタデータの処理、つまり電子通信データが対象となる。ePrivacy規則では、とかくCookieへの影響が取り上げられているが、実際にはCookieは規制対象の一部に過ぎず、チャットや電話、メッセンジャー等のサービス、ダイレクトマーケティングのためのメール送信等も対象だということに留意する必要がある。

地理的範囲と対象により規制適用となった場合、一般企業で影響が大きいと思われる規制内容は以下の条項である。

5条　電子通信データの秘密（＝電子通信事業法でいうところの通信の秘密）

6条　許容される処理（1項に具体的な内容が記載されている）

7条　保存及び消去（特に実務的に影響が大きいと思われるのは2項。通信の伝送の目的に必要がなくなったときには、電気通信メタデータを消去または匿名化しなければならない。）

8条　エンドユーザの端末機器情報の保護（いわゆるCookie規制）

b項で、Cookieはエンドユーザが同意した場合は利用可となっている。また、同意以外で処理可能となるのは、c項でサービス提供に必要とされる場合、d項で視聴者測定の場合としている。ただし、視聴者測定に関しては、サービス提供者自身による処理またはGDPR28条の条件を満たす適切な処理者への委託が条件となっている。なお、GDPR28条の委託は、契約条項まで規定されている点が日本法より厳しい内容となっている。

同意の例外は前文21項に詳しく書かれている。Webサイト関連では、

- 入力フォームのセッション管理のためのCookieは同意が不要
- 認証セッションCookieは同意が不要
- カート内データを引き継ぐために必要なCookieは同意が不要

と明確になっている。

判断が微妙なケースとしては、例えば広告収入で運営されているWebサイトでは、Cookie利用を明確に正確にユーザーフレンドリに情報提供されており、ユーザが受け入れている場合のみ同意が不要となっている。サービス提供に必要な範囲として、場合により広告は入りうるが、その際には明確な情報提供が行われていることが前提となる。また、端末機器そのものを配布している場合は同意が必要となる。

さらに前文21a項にもCookie利用について記載されており、Webトラフィックの計測を匿名で行う

場合は同意不要、ユーザ識別していれば同意必要、セキュリティの修正の場合は同意不要となる。

■同意の取り方

同意の取得方法に関しては、前文 19a 項で、法人へのサービス提供において、取得が必要な同意は法人としてではなく端末のエンドユーザからの同意としている。法人対象のサービス設計でこの同意取得をどのように組み込んでいくかが難しい。この点に関して、前文 20 項で同意取得はサービスプロバイダや ad ネットワークプロバイダ等に委託することも可能としている点が実務を考える上で重要となってくる。

また、前文 20 項 a では同意は必要だが、「同意疲れ」を起こして誰も読まなくなってしまう状況は回避する必要がある。

実例で考える ePrivacy 規則と GDPR

理解を深めるためには、実務上の具体例に当てはめて検討する。例えば、Cookie には、自社サーバーが発行するファーストパーティ Cookie と自社以外が発行するサードパーティ Cookie がある。現在もっともシェアの大きい Google アナリティクスを例にとると、計測のためにユーザに発行される Cookie はファーストパーティ Cookie だが、実際の計測は Google（＝GDPR での処理者）が行っているため自社で個人データ的なものを処理することはなく、統計情報のみが Google から提供される。また非会員制サイトで個人データも保有していない場合、

1）Cookie が個人データに当たらない場合は GDPR 適用外
2）Cookie が個人データに当たる場合、GDPR 適用とはなるが Web トラフィックの統計情報取得であれば Legitimate interests に当たるのではないか
3）GDPR28 条を満たした第三者が処理しているのであれば、ePrivacy 規則の要求としての同意不要ではないか

といったことが考えられる。これに関しては現時点では、そもそも個人データにあたらない Cookie が存在するのかという基本的な部分から現地でも意見が分かれるところなので、一つの捉え方としての例示であり、実際には EU 法の弁護士の助言が必要である。

逆に、広告識別子は個人を識別しうるため、個人データに該当する可能性が極めて高い。同じ Google アナリティクスの利用でも、例えば広告オプションをオンにして広告識別子と紐づけした場合やリマーケティングタグ、コンバージョンタグを設置されている場合は特定の人の行動をトラッキングすることになるため、legitimate interests とは言い難く同意が必要となるのではないか。

以上のとおり、Web トラフィックの計測だけ取ってみても細部の設定により同意取得の必要性が変わるため、実際にどのように運用されているかを確認して判断する必要がある。

さらに、GDPR では広告識別子を取り扱う場合は同意取得に加えて提供先（委託先（処理者を含む））の情報提供義務も発生する。日本法では広告識別子に関しては委託に伴う提供と判断して同意取得していないケースが多いが、GDPR の下では委託先を含む企業名（特定できない場合のみカテゴリ）を記載

する必要がある。なお、日本法では法的には提供先の記載は義務付けられていないが、ガイドライン上、透明性の確保は重要とされている。

寄せられる相談の中には、MA ツールを使用した DM 送信に関するものもあるが、現状行われている施策でも GDPR 対応が難しいと判断されるもの（ビーコンを使った開封確認等）があるので、GDPR 適用されると整理した際は精査する必要がある。

課徴金の事例から考える EU における個人データの保護

■執行状況

EDPB のレポートによると、施行後 1 年間で苦情申し立てが 14.4 万件、データ漏えいの通知 8.9 万件と非常に多く、現地ではプライバシー保護への機運が高まっていると思われる。課徴金の執行も各国で積極的に行われており、少なくとも 11 か国が課徴金を命じ総額で約 70 億円となっている。ドイツでは 2019 年 2 月までに 41 件の課徴金を課している。

■課徴金の実例から見る対応のポイント

1)オーストリア：レストラン（2018 年 9 月）歩道が映る防犯カメラを設置
⇒そのように広範にモニタリングする法的根拠がない、として課徴金約 60 万円

2)ポルトガル：病院（2018 年 7 月）退職した医師のユーザ ID が削除されていない
⇒データ最小化の原則違反　等で課徴金約 5000 万円

3)フランス：Google（2019 年 1 月）課徴金約 63 億円
データ処理の目的、保存期間、広告表示に利用される個人データのカテゴリに関する記載が分割されており容易にアクセスできない　⇒透明性及び情報提供の義務違反
広告パーソナライゼーションのための同意取得が、①十分な情報提供が行われていない、②同意が「specific」でも「unambiguous」でもないため、同意が有効でない　⇒法的根拠がない。
⇒アカウント作成の際に利用規約やプライバシーポリシーへの同意を求めることが、自由意思がなく同意と認められないという点については、現在業界団体等も巻き込み係争中のようである。

4)デンマーク：タクシー会社（2019 年 3 月）顧客情報を 2 年後に匿名化するとしていたが、システムの都合により顧客電話番号を 5 年間保存　⇒　自社システムの都合は GDPR 遵守困難の理由にならない、として課徴金約 2000 万円

5)ポーランド：デジタルマーケティング会社（2019 年 3 月）
公的データベースから 570 万人分のデータを収集し、分析・スコアリング等によるマーケティングサービス提供　⇒　情報提供義務違反として、課徴金約 2700 万円+570 万人への情報提供命令
事業者はメールアドレスがわかる約 68 万人にはメール通知済み+Web サイトに情報掲載済みしていたが、十分でないとの判断

このように、現状では非常に厳しく執行が行われており、調査された際にすべてクリアできている企業は多くないと思われる。調査のトリガーとしては、苦情申し立て、情報漏えい、報道が挙げられるが、リスク管理の観点からは、苦情申し立てされる可能性があるかどうかを検討することが実務的である。こ

れは形式的な話ではなく、GDPR のコンセプトにつながる部分で、苦情申し立てされるということは、インフォームドコンセントができていないということの表れである。

例えば、名刺交換した相手へのお礼メールに苦情申し立てのリスクは感じないが、社内にある数千件のメールアドレスに対し一斉広告メール配信する際に「苦情申し立てがあるかも」と不安に思うのではないか。これは、広告メールの配信にインフォームドコンセントができていない（のでは？）」という認識（＝リスク）があるということである。

また、EU で 14.4 万件の苦情申し立てがあるということは、EU 在住の個人が、日本の個人情報保護委員会に直接苦情申し立て⇒日本当局による調査というケースも想定される。実際に、個人情報保護委員会による執行（報告徴収、指導・助言、立入検査）件数も一昨年と比較し 100 件強増えており、立入検査も 2 件実施されているということを念頭において、形式的ではない「インフォームドコンセント」のあり方を考えていく必要がある。