積極的なデータ活用を見据えた『攻め』と『守り』のプライバシー

TMI総合法律事務所／PwC

「アフターGDPR」における プライバシー保護のグローバリゼーション

1. GDPRを機に厳しくなる各国の個人情報保護法

2018年の欧州一般データ保護規則（GDPR）の施行を機に、各国の個人情報保護法は厳格化の傾向をたどっています。特にブラジル、インド、タイ、日本で施行予定の法令は、GDPRに類似していると言われています。さらに、中国サイバーセキュリティ法や中国個人情報安全規範は、GDPRの影響を受けて個人の権利を強化しています。

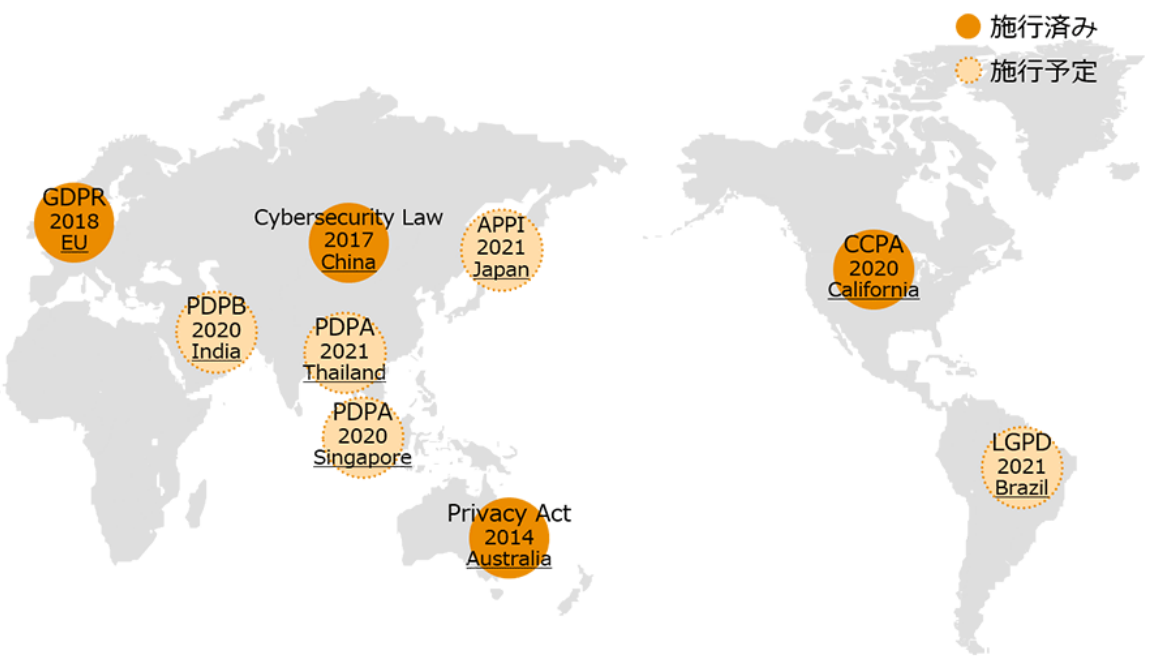
プライバシー保護は元来、1980年に経済開発協力機構（OECD）が策定した「個人情報保護に対する8つの原則」（目的明確化の原則、利用制限の原則、収集制限の原則、データ内容の原則、安全保護の原則、公開の原則、個人参加の原則、責任の原則）が基礎となっています。当原則を礎とし、欧州や日本などでは、EUデータ保護指令、個人情報保護法などが策定されました。

一方、当原則はOECDの加盟国のみに適用され、かつ当原則に対する解釈は、各国に委ねられているため、プライバシー保護のレベルは国ごとに異なりました。特に欧州は、複数の国から成る経済統合体を築いており、これらの国における共通秩序を実現するため、個人情報保護法にも均質性が求められてきました。そこでEU加盟国※1においてプライバシー保護レベルの乖離を平準化するために施行された法令が、GDPRです。

これまでは、個人情報を含む情報を利活用することで新たなビジネスの創出や知見を獲得しようという企業のビジネス上の利益が優先されてきましたが、GDPRの施行を機に、個人情報保護法が厳格化し、ユーザーのプライバシーも尊重されるようになりました。

図1に、GDPRを皮切りに厳格化する各国の個人情報保護法施行の動きをまとめました。これらの法令には、当該国に拠点がない場合にも適用され得る国外適用の要件も含まれています。そのため、グローバルにビジネスを展開する企業は、各国のグループ会社が個別に対策を講じるのではなく、どの法令へも対応できるようにプライバシー保護をグローバライズし、グループ全体へ適用する必要が出てきたと考えられます。

図1：各国で厳格化する個人情報保護法



※1：GOV.UK, “Countries in the EU and EEA”,（2020年8月12日閲覧）

2. プライバシー保護のグローバリゼーションのために企業が行うべき3つの施策

それでは企業は、こうした状況下でどのような施策を講じればよいのでしょうか。実際にプライバシー保護のグローバリゼーションに取り組んでいる企業の事例をもとに説明します。

プライバシー保護施策は一般的に、データマッピング、規程類の策定、グループ管理体制の構築、越境移転への対応、データ主体（ユーザー）の権利への対応、委託先への対応、データ保護影響評価、従業員教育が挙げられます。その中でも特に肝となる論点は、「グローバル管理体制の構築」、「ミニマムのプライバシー保護レベルの設定」、「データマッピングとデータ主体の権利への対応」の3点です。

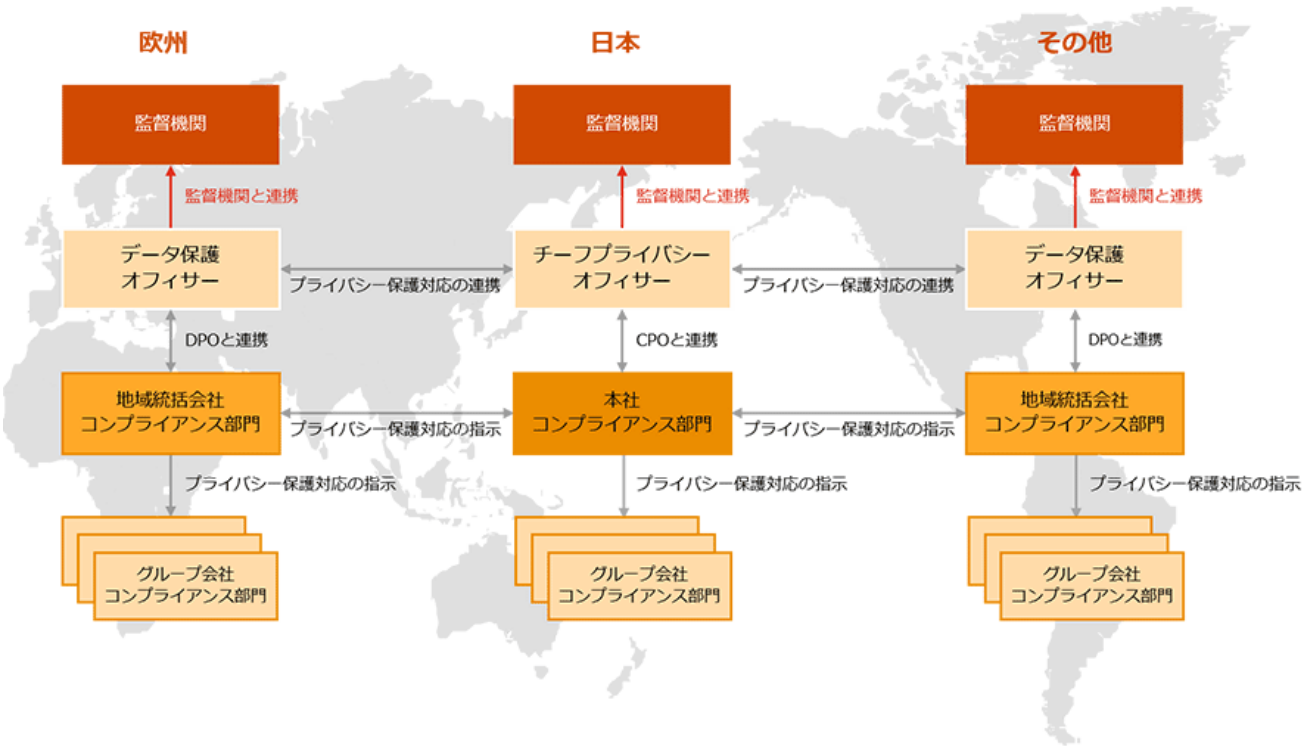
1）各グループ会社が連携するグローバル管理体制の構築

各国の個人情報保護法の動向を把握し、プライバシー保護をグローバライズするためには、まずは各グループ会社が連携を行う管理体制の構築が必要となります。各国の法令下でデータ保護オフィサー（DPO：Data Protection Officer）の設置が求められているか否かに関わらず、企業のビジネス戦略やプライバシー保護へ関与する責任者であるチーフプライバシーオフィサー（CPO：Chief Privacy Officer）やそれを支援するコンプライアンス部門の設置が推奨されます。

既にこうした取り組みを実施している企業は、ビジネスを展開する地域の統括拠点へCPOを設置し、各CPOが担当する地域内のグループ会社のコンプライアンス部門と連携しながら、プライバシー保護に係るアドバイスの提供や監視を行っています。またコンプライアンス部門は、CPOからのアドバイスなどをもとに、プライバシー保護の施策を導入・運用しています。

さらに、全従業員が、CPOやコンプライアンス部門が策定したプライバシー保護に係るルール、体制、運用手順などの情報に対して簡単にアクセスできるように、これらの情報を集約した共有サイトを構築することが推奨されます。

図2：チーフプライバシーオフィサー（CPO）を設置したグローバル管理体制の例



2）ミニマムのプライバシー保護レベルの設定

先に述べたように、各国の個人情報保護法は異なっています。一般的に、欧州、北米、東アジアはプライバシー保護レベルが高く、その他の地域は、未だ途上段階にあると言われています。欧州のGDPRは、プライバシー保護の「グローバルスタンダード」であると言われてはいるものの、当該法令の要件をグループの全拠点へそのまま適用することは、地域特性の違いから難しいでしょう。一方で、多額の制裁を科されるリスクも避けなければいけません。そのため、グローバルにビジネスを展開する企業は、各国の法令の特異性を考慮した上で、ミニマムのプライバシー保護レベルを設定する必要があります。既に取り組みを実施している企業は、自社の地域統括拠点がある国々の法令と要件の差分を把握した上で、独自のグローバルプライバシー保護レベルを設定し、それをもとにグループ会社へプライバシー保護対策を導入・運用しています。

3）グループ内外におけるデータマッピングに基づいたデータ主体の権利への対応

法令の厳格化、データ主体の権利強化に伴い、各国では、ユーザーが個人情報の取り扱いやプライバシーポリシーに係る問い合わせを企業に行うケースが急増しています。実際に、ユーザーからの問い合わせに適切に対応することができず、監督機関から制裁を科されたり、レピュテーションが低下したりした企業も出てきています。

これらのリスクを最小限に抑えるために、企業は、ユーザーから問い合わせを受けた際に、なるべく早く、また正確に応じなければいけません。そのために、企業はグループ内外におけるデータマッピングを行い、自社がユーザーから取得している個人情報の種類、利用目的、適法性の根拠、プライバシーポリシーへの同意の取得状況、第三者提供の状況などを整理しておく必要があります。既に取り組みを実施している企業は、グローバルプライバシー保護レベルをもとに、グループ共通のデータマッピング項目を策定し、CPOや各グループ会社のコンプライアンス部門を通じて、個人情報の取り扱い状況を洗い出しています。

事例において、DMP事業者から広告主に提供されるクッキーIDは、それ単体では特定の個人を識別できる情報ではありません。また、提供元たるDMP事業者においては、特定の個人を識別できる情報は保有していないため、容易に照合できる他の情報と紐づくことによって特定の個人が識別されることもありません。そのため、現行個人情報保護法における「提供元基準説」を前提とした場合、抽出IDの提供は「個人データ」の第三者提供には該当せず、本人の事前同意は不要という結論になります。

しかしながら、改正個人情報保護法26条の2においては、従来の「提供元基準説」を修正する、新たなルールが定められました。この新ルールでは、生存する個人に関する情報であって「個人情報」などに該当しないものが「個人関連情報」と定義されており、提供先が個人関連情報を「個人データとして取得すること」が「想定」される時は、提供元は、当該個人関連情報を提供する前に、本人から同意が得られていることを確認しなければならないとされています。

例えば上の事例で、広告主がDMP事業者から提供を受けた抽出IDを用いて、自らの顧客にダイレクトメールを送付するような場合においては、提供元たるDMP事業者においては個人関連情報に過ぎない抽出IDが、提供先たる広告主においては個人データである顧客管理システム内の情報（氏名、住所など）と紐づけられることになります。これはまさしく、提供先が個人関連情報を「個人データとして取得すること」が「想定」されるケースに該当するはずですから、DMP事業者は、抽出IDの提供に先立ち、ユーザー本人の同意が得られていることを確認する必要があると思われます。

他方で、抽出IDを用いたインターネット広告の配信が広告配信事業者を介して行われる場合で、広告主が抽出IDを自身が保有する顧客データ（氏名など）と紐づけることを予定していないようなときに、一定の条件を満たすことで「個人データとして取得すること」が「想定」されていないと整理し得るのかは、まだはっきりしないところです。

pwc

TMI PRIVACY AND SECURITY

3. グローバライズされたプライバシー保護がビジネスに貢献する

近年、企業の先進的な取り組みとして、合併・買収やジョイントベンチャーの設立などのビジネス戦略と並行して、プライバシー保護のデューデリジェンスを効率的に行う方法を模索しているという例が挙げられます。その取り組みの一つとして、企業は、データマッピングツールやユーザーからの同意状況を管理するコンセントマネジメントツールといったプライバシーテックを採用し、プライバシー保護の柔軟性を高めています。

ビジネスがグローバル化する社会にあっては、企業内のプライバシー保護をグローバライズすることが今後、ますます求められると考えられます。各国の法令に準拠してユーザーの個人情報を適切に管理し、彼らのプライバシーをグローバル規模で保護することが、企業がビジネスを成功させるための礎となるでしょう。GDPRの施行を契機に、こうした取り組みは既に各国で始まっています。

執筆者

大井 哲也

TMI総合法律事務所
TMIセキュリティ＆プライバシー株式会社
弁護士

平岩　久人

PwCあらた有限責任監査法人
パートナー

宮内　美里

PwCコンサルティング合同会社
シニアアソシエイト

PwC Cyber Security & Privacy

https://www.pwc.com/jp/ja/services/digital-trust.html