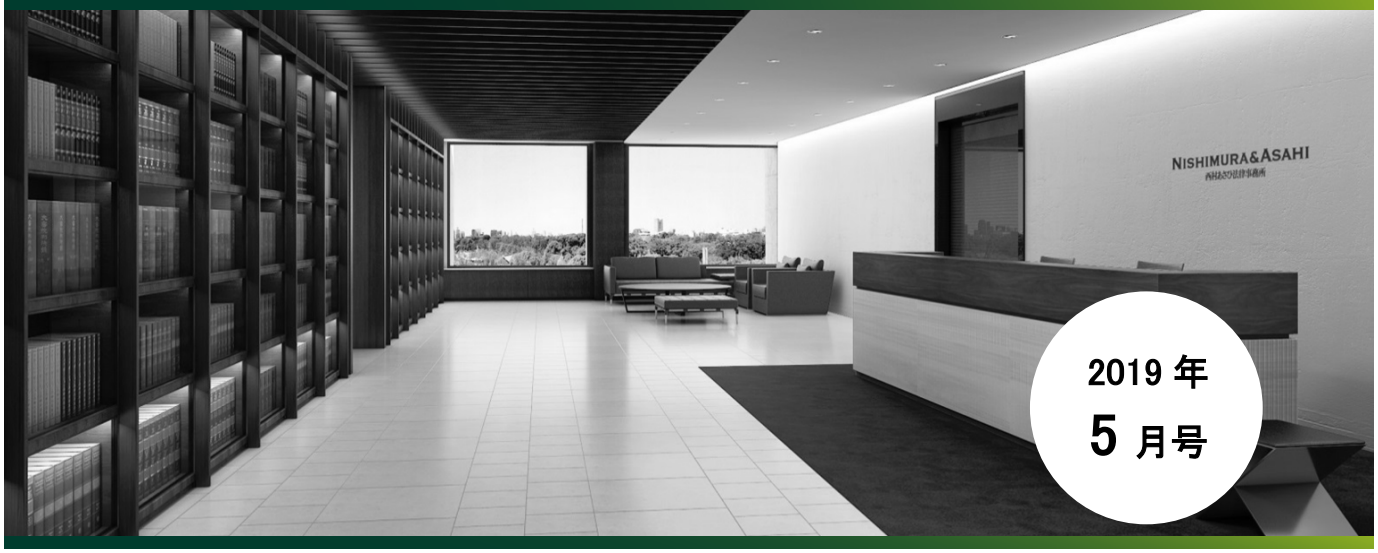
西村あさひ法律事務所
NISHIMURA & ASAHI
ヨーロッパニューズレター



GDPR 施行から 1 年を踏まえての日本企業の対応

執筆者:石川 智也

本ニューズレターでは、2018 年 5 月 25 日の GDPR 施行から 1 年が経過することを踏まえて、今後日本企業が GDPR についてどのように取り組んでいくべきかを概観する。

1. 執行事例の増加

GDPR が施行されてから 1 年が経過し、多くの執行事例が積み上がっている。

日本ではあまり報じられていないが、既に制裁金が課された事例が多く存在するほか、制裁金に至らなくても、当局から連絡が来た事案、監査に至った事案、警告を受けた事案が生じている。決して、大規模なインターネット企業だけがターゲットになっているわけではなく、小規模事業主に対しても着実に執行はなされている。したがって、日本企業の現地拠点での執行リスクは現実的なものである。

特に、制裁金事例は今年に入ってペースを上げて増大してきている。本年 5 月初旬には、制裁金を 2019 年夏に課す旨を公表した監督当局もあり、世界的には話題となった。また、EEA 域外の企業が執行対象になった事例も既に複数存在しており、当分の間は日本企業も含め、EEA 域外の企業が執行の対象にならないというのは、もはや幻想に過ぎない。日本企業についても、制裁金が課された事例は未だ報じられていないが、当局から連絡が来た事案は存在するようである。

執行事例を見ると、

① Privacy Notice の通知を適切に行っていない
② 適法なデータ処理を行っていない(データ処理に関する諸原則を遵守していない、適法性の根拠がない、同意の要件を満たしていない等)
③ 30 条の処理記録を備えていない
④ データ主体の権利行使を尊重していない
⑤ データブリーチの際の通知義務を遵守していない

⑥　セキュリティの水準が不十分である

等の事例が見当たるところである。セキュリティ水準は一朝一夕で解決することが容易でないかもしれないが、それ以外の項目は基礎的なデータマッピングと法定の文書の作成により、短期間で解決できる問題である。費用対効果が議論されることがあるが、執行がなされた場合や、データ漏えい等が生じた場合には、現地の言語で有事対応を迫られる。その際に要する費用は、上記の基礎的なデータマッピングと法定の文書の作成の費用をすぐに超えることになる。

2.　GDPR 対応を一通り終えた企業の今後の対応方針

(1)　アップデート、トレンドのフォロー等の観点

GDPR 対応を一通り終えた企業は、引き続き、①自社グループのデータ処理の発生・変化、②解釈のアップデート、③実務のトレンドの変化をウォッチし、必要な対応を講じていくことが求められる。

①自社グループのデータ処理の発生・変化との関係では、(a)発生・変化を見逃さない態勢整備と、(b)発生・変化が生じたときの適法性の根拠の評価、Privacy Notice の作成・修正、データ処理契約の締結等の対応とが求められる。

②解釈のアップデートについては、欧州データ保護評議会が公表するガイドライン・オピニオンと欧州司法裁判所の判例のフォローが欠かせない。欧州データ保護評議会が今後公表予定としているものの中では、地理的範囲のガイドラインのパブリックコメント後のアップデート、正当な利益に関するガイドライン、管理者と処理者の概念に関するガイドライン、データ主体の権利行使に関するガイドラインは、特に重要性が高いと考えられる。また、欧州司法裁判所の審判対象になっているもののうち、少なくとも、同意の要件が問題となっているもの（C-673/17、C-61/19）、SNS のインタラクションボタンの設置者が管理者になるか否かが争われているもの（C-40/17）、SCC の有効性が争われているもの（T-738/16、C-311/18）は、多くの日本企業の実務に影響があり得る。さらに、自社の拠点のある国の当局が公表するガイドライン・オピニオン及び裁判例、並びに執行の動向についても、フォローが望ましいといえよう。

実際に、ガイドラインの公表によって、従前の実務を変更する必要が生じた項目も少なからず存在する。特に適法性の根拠の評価と、Privacy Notice の項目については、GDPR 施行前と現在とでは実務が異なるものもある。これらについては、前記 1.のとおり執行事例の多い項目であることも踏まえ、GDPR30 条の処理記録とセットで改めて精査を行うことが望ましい。

③実務のトレンドの変化もある。中でも顕著なのは、Cookie への対応を適切に行う事業者が増えたことと、Privacy Notice のトレンドの変化である。Cookie については、当初、システム的な対応の困難さを理由に、分析目的で Cookie を取得する際の同意取得を諦めたり、GDPR の同意の要件を満たさない形でのポップアップを導入するにとどまったりする企業も少なくなかったが、近時は外観上 GDPR の同意の要件を満たしているように思われるものが増えてきている。また、Privacy Notice についても、昨年春頃と比較して、透明性ガイドラインの別添に記載されている注意事項をより忠実に遵守して記載する例が増えてきており、このトレンドの観点からも Privacy Notice の見直しは重要度が高いといえよう。

(2)　グループレベルでの GDPR コンプライアンスの維持のために

グローバルに展開する日本企業にとっては、グループレベルでの GDPR コンプライアンスの維持は、内部統制システムの整備義務の一環として自身の問題として取り組むべき課題である。

グループレベルでの GDPR コンプライアンスを確認・維持する観点からは、GDPR 施行から 1 年を機に GDPR の対応状況に関する監査項目を作成して、グループ会社の監査の際にチェックすることが望ましい。

また、GDPR 施行から 1 年が経過して、担当者の交代に接している企業も少なくない。交代に際しては、十分な引き継ぎを行うことが重要である。その際には、社内セミナーを実施して、今一度担当者の理解を底上げする機会を設けることも有用な方法であり、実際にそのような依頼も多いところである。

3. GDPR 対応が未了の企業の今後の対応方針

(1) EEA 域内にある拠点

EEA 域内にある拠点は、大小にかかわらず、GDPR への対応が必要である。前記 1.のとおり、小規模の事業者であっても制裁金が課された事例が既に発生している。また、B to B のビジネスであっても、従業員の個人データについてはアクセス権等の権利行使や当局への不服申立てが生じやすい類型であるといえる。基礎的なデータマッピングと法定の文書の作成は、執行リスクに照らして費用対効果に欠けるものでは決してないので、可及的速やかに対応に着手することが求められる。

当局による調査では、GDPR30 条の処理記録の提出を求められることが多いほか、少なくとも法定のドキュメント（Privacy Notice、データ処理契約、社内のポリシー、標準契約条項（SCC）など）が提示できないと直ちに GDPR 違反となってしまうため、これらの用意を急ぐ必要がある。また、データ主体による権利行使への対応、データ漏えい等の際の対応の不手際が契機となって監督当局の執行に繋がるケースが多く発生しているため、それらへの対応マニュアルの整備も重要度が高い。

(2) EEA 域外にある拠点

EEA 域外にある拠点にとっては、GDPR のスコープ内のデータ処理があるか否かの評価が不可欠である。この評価に際しては、GDPR のスコープに関する地理的範囲のガイドラインを参照することになるが、実務的には結論を得るのに十分な内容であるとはいえないため、専門家の助言を得て解決する必要がある。

なお、十分性認定により日本企業において GDPR への対応が不要になったというのは誤りである。十分性認定により解決されたのは、EEA 域内から日本への個人データの移転に際して標準契約条項（SCC）の締結等が不要になったという点だけであり、日本企業に GDPR が適用される場合には、引き続き GDPR への対応が必要になる。また、自身に GDPR が適用されない場合であっても、GDPR の適用を受けるデータ処理を受託する場合には、委託元が GDPR を遵守するために所定のデータ処理契約の締結に応じることの検討が必要な場合もある。

4. グローバルでのプライバシー保護コンプライアンスの重要性

世界的にプライバシー保護の機運が高まるとともに、GDPR の影響を受けて、多くの国でプライバシー保護法制が導入・強化されており、グローバルに展開する企業にとっては、各国のプライバシー保護法制に対応することが不可欠な時代となっている。特にリスクの高い法律として認識されているものとして、GDPR の他には、中国のサイバーセキュリティ法、アメリカのカリフォルニア州消費者プライバシー保護法（なお、他の州でも類似の法律の導入に向けた動きがある）があるが、各国拠点における執行リスクという意味では、これらの法律に限らず各国の拠点に適用される法律を確認し、遵守する必要性は高い。

このグローバルでのプライバシー保護コンプライアンスに向けた取組みについても、GDPR 施行から 1 年を機に、近いうちに別のニューズレターで述べたいと考えている。

いしかわ　のりや
石川　智也
西村あさひ法律事務所　パートナー弁護士
n_ishikawa@jurists.co.jp

2006 年弁護士登録。2005 年東京大学法学部卒業、2015 年バージニア大学ロースクール卒業(LL.M.)、2016 年マックス・プランク　イノベーション・競争法研究所併設のミュンヘン知的財産法センター卒業(LL.M.)、Noerr 法律事務所ミュンヘンオフィスに出向、2017 年ニューヨーク州弁護士登録。コーポレート、M&A、IP とデータの保護と利活用に関する法制度を専門とし、グローバルでのデータ規制への対応について多くの日本企業にアドバイスを提供している。情報法制学会会員、Certified Information Privacy Professional/Europe(CIPP/E)。