Information

［セミナーレポート］

緊急開催

GDPR「十分性認定」後の日本企業の情報コンプライアンス対応

登壇者

石川 智也 氏【写真左】（西村あさひ法律事務所 パートナー弁護士）
エリザベス・フォゲッティ 氏（エピック Director,Strategic Relationships & Compliance Consulting）
トーマス・ボンク 氏【写真右】（エピック Vice President,Professional Services）

制作／レクシスネクシス・ジャパン広告出版部

2019年1月23日、欧州委員会は、個人データの保護水準について日本の十分性を認定した。EU一般データ保護規則（GDPR）対応に追われる日本企業にどのような影響を与えるのか。

TOPIC ❶ テクノロジーを駆使した個人情報データ特定を含む情報ガバナンス対応

まず登壇したのは、世界最大級のeディスカバリサービスプロバイダーであり、リーガルサービス業界におけるマーケットリーダーであるエピックのトーマス・ボンク氏と、エリザベス・フォゲッティ氏だ。

「企業には膨大なデータが保有されています。みなさんの会社では、どの場所にどのようなデータが蓄積されているのかを把握できているでしょうか」フォゲッティ氏はこう問いかける。

GDPRでは、データ主体から企業に自身に関するデータについて確認や修正、削除といった権利主張（DSR／DSAR）があった場合、企業は30日以内に応えなければならないとされている。これが実は非常に難しい。「企業には、さまざまな場所に、さまざまなデータが散らばっています。社員個々人に割り当てられたPCや社内サーバー、クラウドなど、どこにどのようなデータがあるのか、しかもその個人に関するデータは一つではないかもしれないし、相当古いものもあるかもしれない。このような中ですべてを洗い出すのは、並大抵のことではありません」（ボンク氏）。「GDPRの法外な制裁金は、漏洩に限ったものではありません。DSARに応えられない場合にも、同様に科されうるのです」（フォゲッティ氏）。

GDPRの成立に端を発し、世界各国ではデータプライバシーに関する規制が強化されている。こうした世界的な流れの中で、両氏は企業における情報ガバナンス強化の必要性を説く。

「GDPRをはじめとした規制に準拠するために企業が取り組むべきは、〝規制を知る（Awareness）〟〝データの所在とリスクを確認する（Discover）〟〝データの管理体制を整え、実践する（Manage）〟〝データを保護する（Protect）〟〝報告の体制を整える（Report）〟の五つのステップです。こうした取り組みは、一部署のみでは不可能です。全社的に、組織横断的なチームを組成して行う必要があります」（フォゲッティ氏）。フランスに拠点を置くとある米国の企業では、当初は法務がGDPR対応を取り組むべきと主張していたCIOも、規制を理解するにつれて率先してこの取り組みに関わるようになったという。

なお、一連のステップの中で、データマッピング同様に重要なのが、文書管理規程や不測の事態における対応プロセスの策定と実践だ。自社がデータを「どこ」に「どの期間」保存するか、あるいはこの原則によらずにデータを保持・削除する場合の判断基準、DSARやデータ漏えい時の対応プロセスを明確に規定し、これを確実に実践する。こうした取り組みは、訴訟に発展した際のeディスカバリにおいても有効だという。

とはいえ、こうした取り組みを自社内だけで行うのは容易ではない。企業の人手には限りがあり、内省には莫大な投資が必要だ。このため、こうした分野に特化した業者にアウトソースしたいと考える企業は少なくない。

GDPRが成立する2016年頃から、エピックでは自社がGDPRに準拠するための取り組みと並行して、事業としてGDPR対応に苦慮する企業にどのようなサポートを提供できるのかを模索し続けているという。「現在、当社ではDSAR対応の自動化（DSAR Administration）や、抽出したPIIの保存や社内データのクラウドへの移管、M&Aにおけるシステム統合、ビジネス上利用価値のなくなった、あるいは規制上保持の対象ではなくなったデータや重複データの整理、業界ごとの規制に沿った文書管理ポリシーの確実な運用、データ漏えい時における発生源や漏洩対象の特定、規制当局やデータ主体への報告・通達といったさまざまな分野で、最先端のテクノロジーを駆使したソリューションを開発しています。GDPRをはじめとする世界的なデータプライバシー規制への対応にお困りの企業のみなさまに、今後も高度なサービスやサポートを提供していきたいと考えています」（ボンク氏）。

TOPIC ❷ 十分性認定後の日本企業の情報法コンプライアンス

「GDPRが適用される企業にとっては、十分性認定後もGDPR対応の必要性は変わりません。また、EUから日本へのデータ移転に際しては、十分性認定に依拠して移転することも、今までどおりSCCに依拠して移転を継続することも可能です」。続いて登壇した西村あさひ法律事務所の石川智也弁護士は、こう語る。

十分性認定による移転と、SCCによる移転には、それぞれメリットとデメリットがある。それを見極めた上での運用が必要なのだと、石川弁護士は指摘する。「例えば移転するデータが一度必ず日本を経由する場合などは、日本の個人情報保護法と補完的ルールを遵守すれば足りる十分性認定に依拠した移転の方が簡単な場合が多いでしょう。一方で、EUから別の第三国に直接移転することもある場合には、従来どおりSCCに依拠して、EUからのデータ移転の根拠を統一する方がグループ全体で見ると簡便な場合も多いです」。既にSCCを締結済みのデータ移転はそのままSCCを、今後の移転には十分性認定を移転の根拠とするハイブリッド型などもあるという。

また、GDPRとの関係で越境移転規制への対応を行っていると、個人情報保護法24条の外国移転規制への対応が未了であることが判明する企業が少なくないと、石川弁護士は指摘する。「日本企業にとって一番重要なのは、やはり日本法への対応です。この機会に、自社が個人情報保護法に準拠したグループ企業へのデータ移転の仕組みを整えているのか確認すべきです」。

GDPRは、その制裁金の高さから最優先で取り組むべきものとして位置付けられているが、そもそもの日本法の対応を疎かにしてしまっては足元をすくわれてしまう。「従業員や取引先の個人情報への対応は適切か、国内であってもグループ会社への個人データの移転は原則として第三者提供に該当し、本人の同意が必要であることをきちんと理解した対応をとっているかなど、専門家の監査を受けて、対応の不備がないかを再確認していただきたいです」（石川弁護士）。

GDPRの成立以降、世界各国でGDPRの内容を参考にした厳格な個人情報保護法制が広がりを見せ、また各国当局が執行を強化する傾向が続いている。またハッキングなどの手法も巧妙化しているため、きちんと対応を行っていたとしても、いつどこで漏洩が発生し、自社が当局の調査対象となってしまうのかは予想がつかない状況だ。

こうした中で日本企業が喫緊の課題として取り組むべき対応として、石川弁護士はグローバルでの情報法コンプライアンスの必要性を指摘する。「当然、すべての国で、すべての項目を一気に対応するのは不可能ですから、まずは自社の拠点がある国について専門家とともに規制内容の初期的な調査を行った上で、リスクベースで対応の優先度を判断して対応のステージに入るべきです。対応の優先度が高い例としては、グローバルでグループ間のデータ共有が行われている場合のデータ移転契約の締結等の対応が挙げられます。また、GDPR以外にも一つ重要な拠点の対応を行うことを通じて、グローバル対応に向けた経験を積むのも一案ではないでしょうか」。