マネジメント講座

個人データ保護 範囲広く

GDPR入門 ③

一般データ保護規則（GDPR）の保護対象となる個人データとは欧州経済地域（EEA）に所在する個人（国籍や居住地などを問わない）を直接または間接的に識別できる情報のことである。氏名や所在地データ、メールアドレスに加え、IPアドレスやクッキーなどのオンライン識別子も対象になる。

日本の個人情報保護法ではオンライン識別子は保護対象には含まれておらず、GDPRの方が広く定義されている。一方、企業などの法人データ、匿名化されたデータは、日本の個人情報保護法と同様に対象外となる。

GDPRではEEA域内に拠点を有しなくてもEEA域内に商品やサービスを提供しているのであれば適用される。つまり、EEA域内で直接ビジネスをしていなくてもショッピングサイトやスマートフォン（スマホ）アプリなどのインターネット取引を介して、EEA所在者の顧客情報を取得・移転してビジネスを展開している場合には、GDPRに準拠した対応を行う必要がある。

GDPRの適用を受ける企業は、「プライバシーポリシーの作成」「GDPRに準拠した同意プロセスの確立」「個人データを処理する委託先との間の契約の確認・見直し」「個人データが侵害された時の監督機関への通知や被害者へ連絡をするための体制整備」などの対応が求められる。ただ実務面から見ると日本の個人情報保護法と類似した対応であってもGDPRの方がより広い範囲もしくは厳しい対応を求めている場合もあるので、社内規定等を検討する際には注意が必要である。

（SOMPOリスクマネジメント取締役　宮崎義久）

GDPRに準拠した対応の例

①プライバシーポリシーの作成
②同意プロセスの確立
③社内規定などの作成
④個人データを処理する委託先との間の契約の確認・見直し
⑤個人データを処理した活動の記録
⑥個人データが侵害した時の監督機関への通知・被害者へ連絡するための体制整備
⑦データ保護影響評価の要否の確認と（必要な場合の）実施
⑧データ保護責任者の要否の確認と（必要な場合の）選任
⑨域外移転規制への対応

SOMPOリスクマネジメント作成

2019年1月8日
日経産業新聞