マネジメント講座

取得には明確な同意必要

GDPR入門 ⑥

個人データを取得する場合、一般データ保護規則（GDPR）ではプライバシーポリシーなどで必要事項を通知すること、同意を取得することが求められるが、その対応方法は日本の個人情報保護法よりも厳格だ。

必要事項の通知では個人情報保護法でも求められる利用目的を通知するだけではなく、データ主体（本人）に利用目的などを示す時、①表示方式は簡潔で、透明性があり、理解しやすく、容易にアクセスできる②文書内容は明確かつ平易な文言を用いることが求められている。これらを前提に本人から個人データを取得する場合、本人以外から個人データを取得する場合、それぞれにおいて必要事項を明記したプライバシーポリシーを本人に通知する必要がある。

本人の同意を取得する場合、本人の積極的な意思表示を示せる仕組みが必要である。暗黙の了解や管理者側で署名などを記載した同意書の作成などは同意とみなされない恐れがあり、必要事項を示した後に同意の意思を確認するチェックボックスを設ける、本人に署名してもらうなどといった措置が必要である。また、本人同意の記録を保管することも求められているため、取得した同意の証跡を改ざんの影響を受けないように適正に保管することも必要である。

同意取得後においても本人が、その同意を撤回できる権利を有していることから、同意取得後においても本人の申し出に応じた適切な対応に向けた体制整備が求められる。そのため、個人データの取得に対しては、プライバシーポリシーの変更といった書面の変更だけにとどまらず、本人の権利の履行に合わせた手順の策定なども求められることになる。

（SOMPOリスクマネジメント取締役　宮崎義久）

個人情報取得において参照すべき主なGDPRの条項

第6条（取扱いの適法性）
第7条（同意の要件）
第12条（データ主体の権利行使のための透明性のある情報提供、連絡及び書式）
第13条（データ主体から個人データが取得される場合において提供される情報）
第14条（個人データがデータ主体から取得されたものではない場合において提供される情報）

（注）SOMPOリスクマネジメント作成

2019年1月29日
日経産業新聞