マネジメント講座

予測される危険性も評価

GDPR入門 ⑤

データ保護影響評価（ＤＰＩＡ）とは、一般データ保護規則（ＧＤＰＲ）で新たに導入されたもので、欧州経済地域（ＥＥＡ）の個人データを取り扱うことに伴うリスクを評価することである。ＤＰＩＡは個人データの取得から廃棄までの各局面の態様を具体的に洗い出し、個人データを処理する際のリスク管理をするためのものである。データを処理する企業側からすると、ＧＤＰＲを順守していることを対外的に説明するためのツールとしても活用できる。

ただし、ＤＰＩＡは全ての企業や処理行為に義務づけられるものではなく、体系的かつ広範囲なプロファイリング（能力や趣向などを評価・予測するために行動履歴データなどを自動化処理により分析すること）を実施したり、センシティブデータ（人種・政治・病歴など）を大規模に処理するなど、個人データを取り扱うことによって高度のリスクをもたらす可能性がある場合には実施が求められている。自社で取り扱う個人データの処理行為がＧＤＰＲで定める実施義務の判断基準に照らして実施の該非を判断することになる。データ処理をする際に新しい技術を導入する場合にはＤＰＩＡの実施が推奨されている。

ＤＰＩＡはＧＤＰＲの適用対象となる個人データが自社でどのような処理行為をしているのかを把握することの第一歩になり、適切にリスク管理をするための入り口といえる。

そのため、ＧＤＰＲで求める実施基準にかかわらず、適切なリスクコントロールが講じられているか確認するＤＰＩＡの仕組みを導入し、定期的に個人データの取り扱い状況を評価することが重要である。

（ＳＯＭＰＯリスクマネジメント取締役　宮崎義久）

ＤＰＩＡを実施する際に含める事項

- 想定されるデータ処理業務の内容およびその目的
- 目的に対するデータ処理業務の必要性
- データ処理することによって想定されるリスクの大きさ（程度）
- 上記リスクに対処するために講じる対策

（ＳＯＭＰＯリスクマネジメント作成）

2019年1月22日
日経産業新聞