

個人情報保護法への対応について

HVG法律事務所 Saskia Vermeer de Jongh (CIPP/E and CIPP/M)、長谷川 弓



御社では、現地従業員の年齢や給与などの人事データや、顧客リスト、または個人の医療に関するセンシティブデータ(機微情報)等を日本の本社と共有されたりしていませんか？

日本でも昨年9月、情報漏えいに対する罰則を含む改正個人情報保護法が成立しましたが、EUでもEUデータ保護「指令」(EU Data Protection「Directive」)と現在呼ばれているものが、2018年にはEU加盟各国統一法形式としての「規則」(EU General Data Protection「Regulation」)となり、個人データの保護が個人の基本的権利として明記されるなどより厳しい法律になります。

EUデータ保護規則の主なポイントの一つは、たとえ同じ会社の本社と子会社の間であっても、EU外の会社と個人情報をシェアすることは罰則の対象になることです。

プライバシー・シールド(Privacy Shield)規則を持つ米国や、スイス、カナダのように欧州委員会によって例外措置を取られている国と違い、日本は個人情報に関して「十分なレベルの保護措置(adequate level of protection)を確保していない国」とみなされているため、オランダの日系企業が日本の本社へ個人情報を送りたい場合、会社間で基本契約を結ばなくてはならないなど特別な注意が必要です。

本稿では、オランダ・EUにおける個人情報保護法に関する最新の動向と注意点をお伝えします。

背景

オランダデータ保護法

(Dutch Data Protection Act, DDPA. オランダ語ではWet bescherming persoonsgegevens)

オランダでは、1995年以降、個人情報(特定された、または特定しうる個人に関するあらゆる情報)の保護はオランダデータ保護法によって管理されており、オランダにある全ての日系企業も適用対象となっています。

オランダデータ保護法は2016年1月1日に改正されました。最も重要な改正点は、ほとんどのデータ保護法違反が罰金につながる可能性があり、その罰金額は最大EUR820,000、またはその会社の年間売上高の10%となったことです。

また、各企業は、個人情報のセキュリティに関する全てのインシデントの記録を保管することが義務付けられました。

さらに、情報漏えいがあった場合、オランダデータ保護局(Dutch data protection authority)と情報が漏えいした個人(情報漏えいが悪影響を及ぼすであろう個人)に、速やかに報告しなければならなくなりました。

EU一般データ保護規則

(EU General Data Protection Regulation, GDPR)

2018年上半年期にはEU一般データ保護規則(GDPR)が施行される見込みで、その時点でオランダデータ保護法はEU一般データ保護規則にとって代わられます(28のEUメンバー国に同時に適用されます)。EU一般データ保護規則の最終的な草案は、3年間の立案及び審議期間を経て欧州議会と欧州連合理事会によって2015年12月15日に非公式に合意され、内容もほぼ最終になっています。

本規則の目的は、個人の情報保護に関する権利を強化し、EUデジタル単一市場での個人データの自由な流れを促進すること、そして事務負担を軽減することにあります。

EU一般データ保護規則は、EU域内に事業所がある、またはEU域内居住者に商品やサービスを提供している、またはその行動様式をモニタリングしている、全ての日系企業にも適用されます。

情報漏えいに関してもオランダデータ保護法と同様の通知義務が設けられる予定ですが、不履行の場合の罰金はより高額になり、最大でEUR20,000,000、またはその企業の世界年間売上高の4%にもなる見込みです。