GDPR hits us all

Anja Dekhuijzen houdt zich als vooraanstaand advocaat bij Whitebridge bezig met IT- en outsourcing. Ze adviseert in die hoedanigheid cliënten over vraagstukken rondom outsourcing, IT-contracten, IT-disputen, telecommunicatie, e-commerce en privacy.

Gefeliciteerd! U hebt een nieuwe baan. Voor het eerst in uw leven bent u werkzaam voor een IT-vendor. En daar wordt u meteen belast met het security- en privacybeleid van het bedrijf. Hoe pakt u dit aan?

U weet dat datalekken op dit moment al kunnen worden beboet in Nederland. Maar wat volstrekt nieuw is onder de Europese privacywet, die op 25 mei 2018 van kracht wordt in de hele EU en onze Nederlandse wetgeving vervangt, is dat voor het eerst IT-vendors in hun rol als bewerker van persoonsgegevens rechtstreeks door de Autoriteit Persoonsgegevens kunnen worden aangesproken en boetes opgelegd kunnen krijgen. Zo zijn bewerkers vanaf volgend jaar wettelijk verplicht om datalekken onverwijld door te geven aan hun klanten (de verantwoordelijken van de persoonsgegevens). Ook zijn ze wettelijk verplicht afdoende securitymaatregelen te nemen bij de bewerking. Daarnaast gaat uw bedrijf wettelijk direct vallen onder de restricties voor crossbordertransfers van persoonsgegevens, namelijk alleen naar landen die volgens de GDPR een adequaat beveiligingsniveau hebben geregeld in de wet. En dit is slechts een kleine greep uit de verplichtingen die op de bewerkers komen te rusten.

Dat deze verplichtingen beslist geen wassen neus zijn, blijkt uit het feit dat vanaf 25 mei 2018 bewerkers van persoonsgegevens direct boetes opgelegd kunnen krijgen voor niet-nakoming van de GDPR. Die boetes kunnen oplopen tot 20 miljoen euro per gebeurtenis, of 4 procent van de totale wereldwijde omzet (de hoogste van de twee!). Dit betekent onvermijdelijk dat IT-vendors een nieuwe strategie zullen moeten invoeren voor wat betreft het aangaan van verplichtingen, in bijvoorbeeld cloudcontracten, IT-contracten en outsourcingsdeals wanneer daarbij de verwerking van persoonsgegevens is betrokken. En aangezien contracten die op dit moment worden gesloten doorgaans over een jaar nog geldig zijn, betekent dit dat nu al vooruitlopend op de GDPR de IT-contracten, waaronder de 'data processing agreement' (DPA), de bewerkersovereenkomst, hierop moeten worden aangepast.

Deze nieuwe verscherpte privacyregelgeving voor IT-bedrijven zal ook impact hebben op de klanten. Veel meer dan voorheen zal moeten worden nagegaan of de beoogde IT-vendor kan voldoen aan de nieuwe eisen die de GDPR aan hem stelt. Zoals bekend worden ook de boetes aan klantzijde sterk verhoogd onder de GDPR. Daar waar nu in Nederland reeds een boete geldt voor datalekken, geldt deze boete direct in de hele EU. Bovendien kunnen ook aan klantzijde boetes vallen tot 20 miljoen euro of 4 procent van de totale wereldwijde omzet voor allerlei overtredingen van de GDPR. Het is voor klanten van belang dat zij contractueel met hun IT-vendor afspreken dat een boete kan worden verhaald op de IT-vendor wanneer deze de facto verantwoordelijk is voor de niet-nakoming. Dit geldt niet alleen voor nieuwe contracten. Ook bestaande contracten zullen hierop moeten worden doorgelicht.

Interessant in dit geheel is hoe het Verenigd Koninkrijk (VK) zal varen onder de Brexit. Premier May heeft in haar brief geschreven dat zij bestaande Europese regelgeving wil handhaven. Hier zou in principe ook de huidige Europese privacywetgeving onder vallen. Echter, de GDPR is nieuwe wetgeving en zal dus wellicht niet worden ingevoerd in het VK. Dit kan tot gevolg hebben dat het VK niet langer een land is waarnaar men kan worden geacht persoonsgegevens uit te voeren, omdat het VK niet langer een adequaat beveiligingsniveau zou hebben onder de GDPR. Dit betekent dat nu al veel bedrijven zich afvragen of het nog wel verantwoord is om gegevens te laten bewerken in het VK. We zullen scherp in de gaten houden hoe deze situatie zich ontwikkelt. Er is werk aan de winkel. Time to act!