DOOR ANJA DEKHUIJZEN

MOGELIJKE WEEFFOUT IN GDPR VORMT ONVOORZIEN RISICO

Op 25 mei 2018 gaat de nieuwe Europese privacywet gelden, de GDPR. Deze vervangt de huidige Nederlandse privacywetgeving. De GDPR richt zich op privacybescherming van natuurlijke personen. Hiertoe worden voor het eerst in de geschiedenis miljoenenboetes in de wet opgenomen.

ANJA DEKHUIJZEN IS PARTNER BIJ WHITE-BRIDGE ADVOCATUUR EN GESPECIALISEERD IN IT, OUTSOURCING EN PRIVACY.

Deze boetes betreffen bedragen tot 10 miljoen euro voor een aantal overtredingen, waaronder datalekken. Een nog hoger boeteregime van 20 miljoen euro wordt geïntroduceerd voor fundamentele basisprincipes, zoals toestemming en de rechten van de natuurlijke personen.
Dat het menens is, blijkt uit de recent vastgestelde Guidelines van de Artikel 29-werkgroep van de EU betreffende deze boetes. Hierin wordt benadrukt dat de boete van 10 miljoen voor datalekken kan worden opgehoogd tot 20 miljoen: "*This would be likely to be the case where such breaches have previously been addressed in an order from the supervisory authority, an order which the controller or processor failed to comply with.*" Voorts wordt duidelijk aangegeven, anders dan hier en daar wordt gesuggereerd, dat de boetes niet slechts als laatste redmiddel fungeren: "*The point is to not qualify the fines as last resort, nor to shy away from issuing fines, but on the other hand not to use them in such a way which would devalue their effectiveness as a tool.*" De Guidelines bevestigen dat het uiteindelijk aan de nationale rechter is, om te beoordelen of een door de Autoriteit Persoonsgegevens opgelegde boete terecht is.

Subverwerker

Men zou verwachten dat de GDPR bedrijven (en overheden) maximaal in staat stelt om boetes te voorkomen. Dit lijkt evenwel niet het geval. Veel bedrijven besteden de verwerking van persoonsgegevens uit aan een ander bedrijf, de verwerker. Deze verwerker heeft vaak op zijn beurt een zogeheten subverwerker in de arm genomen, die de daadwerkelijke verwerking uitvoert. Deze subverwerkers zijn vaak grote, internationale bedrijven. De GDPR verplicht je als bedrijf zelf het datalek te melden, ook indien dit bijvoorbeeld is veroorzaakt door de subverwerker. Je loopt als bedrijf zelf het risico hiervoor een boete te krijgen. Hier zit hem nu de kneep. Om het datalek goed te kunnen melden aan de Autoriteit Persoonsgegevens, én de boete te kunnen verhalen, zul je op de hoogte moeten zijn van wat er bij de subverwerker gebeurt en wat ermee is afgesproken. Maar de GDPR voorziet niet in een recht op inzage door het bedrijf op wat er is afgesproken tussen de verwerker en de sub-verwerker. Sterker nog, hier zit vaak geheimhouding op.
Ook het voorkómen van een datalek door een subverwerker is hiermee lastig(er). Weliswaar geeft de GDPR aan dat de verwerker in het contract met de subverwerker moet opnemen dat er voldoende waarborgen zijn rond de verwerking van persoonsgegevens, maar als bedrijf heb je geen enkele invloed op de naleving hiervan. In de GDPR is geregeld dat uiteindelijk de verwerker jegens het bedrijf aansprakelijk blijft voor nalatigheden door de subverwerker. Dit is niet zonder risico's. De GDPR kent niet voor bedrijven een eigen rechtstreekse claimmogelijkheid op de subverwerker. Wanneer je als bedrijf zelf de boete opgelegd krijgt, zul je moeten zien of je deze op de verwerker (de tussenschakel) kan verhalen, welke mogelijk financieel zal omvallen. Bovendien is het vaak lastig de aansprakelijkheid van de subverwerker aan te tonen, aangezien je geen achterliggende informatie of afspraken kent.

Aansprakelijk

De opstellers van de GDPR hebben weliswaar gemeend bedrijven te beschermen door de verwerker als hoofdaansprakelijke aan te stellen, maar nu in de praktijk vaak juist de subverwerkers de grote partijen zijn, ontstaat hier wel degelijk een risico. Immers, als bedrijf loop je het risico een boete opgelegd te krijgen, waarbij het lastig is om deze op de daadwerkelijke veroorzaker te verhalen. *