DOOR ANJA DEKHUIJZEN

IEDEREEN WORSTELT MET DEADLINE INVOERING GDPR

De invoering van de nieuwe Europese privacywet, de GDPR, nadert met rasse schreden. Vanaf 25 mei 2018 zal de EU de hoogste privacybescherming ter wereld hebben. Om nakoming van deze wet af te dwingen, gelden voor het eerst in de geschiedenis miljoenenboetes.

ANJA DEKHUIJZEN IS PARTNER BIJ WHITEBRIDGE ADVOCATUUR EN GESPECIALISEERD IN IT, OUTSOURCING EN PRIVACY. WHITEBRIDGE IS UITGEROEPEN TOT PRIVACY LAW FIRM OF THE YEAR 2018 IN THE NETHERLANDS.

Voor veel bedrijven en organisaties is het een race tegen de klok om tijdig GDPR-compliant te zijn. De EU c.q. de Europese toezichthouders lijken zelf niet tijdig klaar te zijn. Zo zijn de GDPR-guidelines van de Europese toezichthouders (waaronder de Nederlandse Autoriteit Persoonsgegevens – de AP) nog niet allemaal af. Er circuleren een aantal *draft-guidelines* waarvan niet duidelijk is wanneer deze worden gefinaliseerd en wat er nog gewijzigd zal worden.
Een tweede probleem betreft de strenge boetes op het ongeoorloofd uitvoeren van persoonsgegevens buiten de EU en datalekken. Zoals in mijn vorige column werd beschreven is dit een heikele kwestie, omdat in de praktijk de verwerking van persoonsgegevens vaak door de processor (uw bewerker) wordt uitbesteed aan grote buitenlandse partijen, de zogeheten subprocessors. Dit zijn partijen waarmee niet uw organisatie zelf, maar uw processor het contract heeft. De GDPR geeft u niet het recht op inzage in de contracten met de subprocessors. Dit terwijl bijvoorbeeld datalekken vaak bij de subprocessor kunnen plaatsvinden, omdat zij de feitelijke verwerking doen. Als bedrijf loop je het risico zelf hiervoor een boete te krijgen. Naar verluidt overweegt de EU om zogeheten 'model clauses' op te stellen, die de transfer van persoonsgegevens buiten de EU regelen tussen uw processor en de subprocessor. Dit zou de huidige wildgroei aan afspraken met subprocessors (vaak gedicteerd door de subprocessor) kunnen indammen. De EU heeft al soortgelijke model clauses opgesteld in andere relaties zoals 'controller to controller'. Voordeel van dergelijke stukken is dat het dan door de EU opgestelde en goedgekeurde voorbeeldcontracten betreft. Echter, een dergelijk stuk ontbreekt tot op heden.

Huiswerk

Ook de Nederlandse AP heeft nog huiswerk te doen. Zo schrijft art. 35 lid 4 GDPR voor dat de AP een lijst opstelt met verwerkingen waarvoor verplicht een DPIA (privacy impact assessment) moet worden uitgevoerd door bedrijven en organisaties voordat de verwerking mag plaatsvinden. Tot op heden (3 april 2018) vermeldt de AP op haar website dat deze lijst er nog niet is.
Een mogelijke weeffout in de GDPR maakt verder dat ook overheden uitstelgedrag vertonen. Iedere lidstaat mag belangrijke aanvullende wettelijke privacyeisen stellen. Echter, conform de GDPR hoeft deze wetgeving pas 25 mei 2018 gereed te zijn. Waarom mogen de lidstaten tot een dergelijke late datum nog wetgeving implementeren? Weliswaar zal deze wetgeving niet met terugwerkende kracht worden ingevoerd, maar onduidelijk is nu waar men aan toe is. De realiteit is dat recent nog Kamervragen werden gesteld over het nut van dergelijke aanvullende wetgeving.
Voor de diverse wetgevers, en in hun kielzog de supervisory authorities, lijkt het een heidens karwei om tijdig gereed te zijn voor de GDPR. De Article 29 Working Party-guidelines over de boetes zijn wel al gereed. Hierin wordt gesteld dat men het boeteregime ook daadwerkelijk zal gaan handhaven. In Nederland heeft minister Dekker recent aangegeven dat handhaving van de GDPR wellicht iets zal worden uitgesteld. Dekker gaf hierbij aan dat het laatste woord hierover bij de AP blijft. Met andere woorden: er is geen zekerheid dat dit uitstel zal worden gehandhaafd. Onder de streep blijkt de gang van zaken een extra hindernis die organisaties moeten nemen om GDPR-compliant te worden. *