MIRJAM ELFERINK EN MARTIJN KORTIER

Binnen enkele jaren gaat de Europese Algemene Verordening Gegevensbescherming in. Nieuwe regelgeving ter bescherming van persoonsgegevens, waar vrijwel ieder bedrijf mee te maken krijgt.

Bent u er klaar voor?

De nieuwe Europese privacyregels

Als bedrijf heeft u al snel te maken met persoonsgegevens. Gegevens van en over uw (potentiële) klanten en medewerkers kunnen bijvoorbeeld persoonsgegevens zijn. Als u die gegevens op enigerlei wijze verwerkt - bijvoorbeeld door ze op te slaan op uw systemen, ze te gebruiken voor direct marketing of voor het verzenden van producten – bent u aan te merken als 'verantwoordelijke' in de zin van de Wet bescherming persoonsgegevens (Wbp).

U bepaalt immers, zoals de wet dat definieert, het doel en de middelen van die verwerking. Als uw bedrijf dan verantwoordelijk is voor de verwerking van persoonsgegevens, en waarschijnlijk is dat dus het geval, dan is het volgende mogelijk voor u van belang. De EU wil de privacy van Europese burgers beter beschermen via een nieuwe Algemene Verordening Gegevensbescherming (AVG).[1]

Het Europees Parlement heeft hier recentelijk een voorstel voor aangenomen. Deze verordening bepaalt onder meer dat organisaties bij het niet tijdig melden van een datalek een geldboete opgelegd kunnen krijgen tot 2% van de wereldwijde jaaromzet. Maar de verordening regelt meer. In dit artikel behandelen wij in een notendop een aantal speerpunten van de conceptverordening.

Wanneer de Raad van de Europese Unie akkoord gaat met het voorstel voor de privacyverordening wordt deze van kracht. Het bijzondere van een verordening is dat hij rechtstreekse werking heeft. Dit betekent dat een verordening niet hoeft te worden omgezet in nationale wetgeving. Met andere woorden: de regels zullen dan per direct gaan gelden in alle Europese lidstaten. Bovendien gaat de verordening voor op de nationale privacywetgeving.

Wat regelt de verordening?

De conceptprivacyverordening bevat een aantal verdergaande wijzigingen ten opzichte van de huidige EU-wetgeving. Hierna geven wij enkele voorbeelden.

1 Functionaris voor de gegevensbescherming

Nieuw is dat organisaties in sommige gevallen verplicht worden om een interne functionaris voor de gegevensbescherming aan te stellen. Dat is op grond van de huidige Nederlandse wetgeving nog facultatief. Is uw bedrijf verantwoordelijk voor persoonsgegevensverwerking en bent u:

- een overheidsinstantie,
- een onderneming met meer dan 250 werknemers of
- bestaat de *core business* van uw organisatie uit het verwerken van persoonsgegevens ?

Dan bent u in de toekomst gehouden een functionaris voor de gegevensbescherming aan te stellen.

2 Recht om vergeten te worden en het recht om gegevens te laten wissen

Betrokkenen hebben onder bepaalde voorwaarden het recht dat de verantwoordelijke ervoor zorgt dat zijn persoonsgegevens worden gewist en verdere verspreiding van dergelijke gegevens achterwege blijft. Overigens bepaalde het Europese Hof van Justitie op 13 mei jl. in een kwestie tussen een Spaanse burger en Google dat Google op verzoek links in de zoekresultaten naar personen moet verwijderen, omdat Europese burgers het recht hebben om vergeten te worden. Google heeft recentelijk zijn beleid hierop al aangepast. Zo kunnen betrokkenen via een webformulier aan Google verzoeken om hun gegevens te laten verwijderen.

3 Recht van gegevensoverdraagbaarheid

Betrokkenen krijgen tevens een recht op gegevensoverdraagbaarheid. Dit houdt in dat betrokkenen mogen verzoeken om hun persoonsgegevens van het ene elektronische verwerkingssysteem naar het andere over te (laten) dragen zonder dat de verantwoordelijke dat kan belemmeren. De verantwoordelijke is hierbij verplicht om deze gegevens te verstrekken in "een elektronisch en gestructureerd formaat dat algemeen wordt gebruikt en door de betrokkene kan worden gebruikt."

4 Expliciete toestemming vereist

Als algemeen uitgangspunt geldt dat betrokkenen toestemming moeten geven voor de verwerking van persoonsgegevens. Dit geldt tenzij een andere wettelijke verwerkingsgrondslag van toepassing is. De verordening eist nu dat deze toestemming "uitdrukkelijk" zal worden verleend. De betrokkene dient zich ervan bewust te zijn waarvoor hij precies toestemming geeft. Concreet betekent dit bijvoorbeeld dat niet in algemene voorwaarden mag worden opgenomen dat de wederpartij toestemming geeft voor de verwerking van zijn persoonsgegevens. Een dergelijke toestemming zal immers niet als uitdrukkelijk kunnen worden aangemerkt.

5 Meldplicht datalekken

Wanneer sprake is van "inbreuk in verband met persoonsgegevens" – in de volksmond ook wel datalek - moet dit binnen 24 uur worden gemeld aan de toezichthouder. Dit geldt tenzij dat redelijkerwijs niet mogelijk is. Onder "inbreuk" wordt verstaan: een inbreuk op de beveiliging met de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig, tot gevolg. Daarnaast moet ook de betrokkene zelf worden ingelicht, indien het waarschijnlijk is dat het datalek de bescherming van de persoonlijke levenssfeer van de betrokkene nadelig beïnvloedt. De toezichthouder kan bij het nalaten van de melding waar dat wel had gemoeten een geldboete tot één miljoen euro opleggen of, bij een onderneming, een geldboete van 2% van de wereldwijde jaaromzet .

Ook op nationaal niveau zijn wettelijke maatregelen voorgesteld om eventuele schade van datalekken te beperken c.q. te verminderen. Over het wetsvoorstel 'meldplicht datalekken' schreven wij eerder in het Huisorgaan van het Platform voor Informatiebeveiliging.[2]
In dit wetsvoorstel wordt een meldplicht voorgesteld in het geval zich een 'datalek' heeft voorgedaan.

1 Voorstel voor een verordening van het Europees Parlement en de Raad, Brussel, 25 januari 2012.

2 Huisorgaan van het PvIB, nummer 7, 2012.

"Een datalek moet binnen 24 uur gemeld worden aan de toezichthouder."

"Voorkom hoge boetes doordat u de nieuwe regelgeving niet kent."

Voor wie gaat de meldplicht gelden?

De meldplicht gaat gelden voor de verantwoordelijke, als eerder gezegd dus degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (definitie Wbp). Een werkgever is bijvoorbeeld aan te merken als een verantwoordelijke. Onder het begrip verwerking valt elke handeling die betrekking heeft op persoonsgegevens, van het moment van verzameling tot vernietiging. Daaronder valt ook het opslaan van gegevens door een derde. Wanneer een onderneming bijvoorbeeld zijn personeelsadministratie uitbesteedt aan een bureau dat zich volledig onderwerpt aan de instructies van de desbetreffende onderneming en uitsluitend onder diens verantwoordelijkheid gegevens verwerkt, is eveneens sprake van bewerkerschap.

De meldplicht zal worden opgenomen in de Wbp. Vanwege privacyoverwegingen moeten betrokken personen in zo'n geval snel worden ingelicht. Dit betekent dat organisaties worden verplicht diefstal, verlies of misbruik van persoonsgegevens te melden aan de betrokken personen en aan het College Bescherming Persoonsgegevens (CBP). Het wetsvoorstel tot wijziging van de Wbp regelt dat niet elke inbreuk op persoonsgegevens hoeft te worden gemeld, omdat niet elk risico een melding rechtvaardigt. Maar hoe weet een verantwoordelijke wanneer hij wel of niet hoeft te melden?

Wanneer is sprake van een datalek?

Staatssecretaris Teeven heeft onlangs een wijziging[3] voorgesteld van het Nederlandse wetsvoorstel 'meldplicht datalekken' dat hierover meer duidelijkheid zou moeten scheppen.[4] De kern van zijn voorstel is dat niet "alle" inbreuken op de beveiliging van persoonsgegevens bij het CBP hoeven te worden gemeld, maar alleen die datalekken die "ernstige" nadelige gevolgen hebben voor de bescherming van de verwerkte persoonsgegevens. Het is maar zeer de vraag of deze wijziging wel strookt met de verplichting uit het voorstel voor de Privacyverordening die een melding aan de toezichthouder vereist in geval van een "inbreuk in verband met persoonsgegevens". De meldplicht geldt niet indien de verantwoordelijke c.q. bewerker passende technische beschermingsmaatregelen heeft/hebben genomen waardoor de betreffende persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden die geen recht hebben op kennisname hiervan.

Wat staat verantwoordelijken te doen?

Het is zaak dat u als verantwoordelijke voor de persoonsgegevensverwerking processen en mechanismen gaat inrichten in uw organisatie, voor zover u dat nog niet heeft gedaan – opdat u kunt voldoen aan de vereisten van de Privacyverordening die binnen nu en enkele jaren in werking zal treden. Door nu al processen te standaardiseren en een functionaris voor de gegevensbescherming aan te stellen die verantwoordelijk is voor de omgang van en met persoonsgegevens binnen uw organisatie loopt u in de pas met de toekomstige wetgeving. Voorkom hoge boetes, doordat u niet op de hoogte bent van de nieuwe Europese wet- en regelgeving!

U zou kunnen denken aan het opstellen van een privacyprotocol waarin wordt geprotocolleerd hoe om te gaan met persoonsgegevensverwerking en wat te doen in geval van calamiteiten. U beperkt daarmee risico's en maakt uw organisatie bewust van de gevoeligheid van de omgang met precaire gegevens.[5] ■

Mirjam Elferink en Martijn Kortier zijn advocaat bij KienhuisHoving Advocaten en Notarissen. Martijn is daarnaast gastdocent Recht bij Saxion.

3 Nota van wijziging bescherming persoonsgegevens 33662.

4 Lees over de laatste stand van zaken: Nota naar aanleiding van het verslag Wetsvoorstel meldplicht datalekken, 7 mei 2005.

5 Over een dergelijke protocol schreven wij eerder in het Huisorgaan van het Platform voor Informatiebeveiliging Huisorgaan van het PvIB, nummer 7, 2012.