Be aware and prepare: de Algemene Verordening Gegevensbescherming

Auteur: Linda van der Niet

Het risico dat persoonsgegevens op straat komen te liggen is vandaag de dag vele malen groter dan 20 jaar geleden. Talloze voorbeelden van gelekte persoonsgegevens komen in de media voorbij, vaak door gebruik van digitale media en producten. Naar aanleiding van deze digitalisatie is door de Europese Commissie en het Europees Parlement besloten aan de privacywetgeving in Europa te sleutelen, teneinde deze verder te ontwikkelen en te uniformeren. Vóór 25 mei 2018 dienen verwerkers van persoonsgegevens compliant te zijn met de nieuwe wetgeving, aldus adviseren wij: Be aware and prepare!

Achtergrond en scope

De privacy van persoonsgegevens in Europa werd tot nu toe beschermd door de Privacy Richtlijn uit 1995 (Rl 95/46/EG). De nationale wet- en regelgeving van de lidstaten is op deze richtlijn gebaseerd. In Nederland is de richtlijn geïmplementeerd via de Wet bescherming persoonsgegevens (Wbp). Doel van deze richtlijn is de rechten en vrijheden van Europese burgers te beschermen bij de verwerking van persoonsgegevens.

Op 25 mei 2016 is de Algemene Verordening Gegevensbescherming (AVG) vastgesteld en deze zal op 25 mei 2018 in werking treden. De AVG heeft de status van verordening en is daarom rechtstreeks van toepassing in de nationale wet- en regelgeving. Implementatie is in principe overbodig geworden waardoor sprake is van een meer uniforme Europese regeling. Er is nog wel een mogelijkheid tot interpretatie naar eigen behoefte; in Nederland zal dit proces waarschijnlijk via de Autoriteit Persoonsgegevens (AP) lopen. De ratio achter de invoering van de AVG is de versterking en uitbereiding van privacy rechten, meer verantwoordelijkheden voor organisaties en dezelfde, uitgebreide bevoegdheden voor alle Europese toezichthouders.

Hoge boetes en toezicht op naleving

Het toezicht onder de Wbp wordt in Nederland bewerkstelligd door de AP. Op dit moment kunnen boetes oplopen tot € 820.000,00 of 10% van de jaaromzet. Vaak zal de AP eerst een waarschuwing/bindende aanwijzing afgeven en aan te brengen verbeteringen controleren. In beginsel mag zij direct een boete opleggen als de verantwoordelijke verwerker opzettelijk of grof nalatig heeft gehandeld. De AP kan na invoering van de AVG nog steeds, en soms meer ingrijpend waarschuwen, berispen, bevelen geven,

verwerkingsverboden opleggen en rectificatie of wissen bewerkstelligen. Ook is het voor haar mogelijk na 25 mei 2018 sneller en vooral hogere boetes op te leggen aan zowel verantwoordelijken als derden verwerkers. De AP (en alle andere toezichthouders binnen Europa) kan bij schending van materiële aard die de privacy van betrokkene direct raakt boetes opleggen tot € 20.000.000,00 of 4% van de wereldwijde jaaromzet. Ook kan zij dezelfde boete opleggen als haar bevel niet wordt opgevolgd. De AVG kent geen formele drempel meer om boetes op te kunnen leggen.

Op dit moment is het toezicht op naleving nationaal geregeld door implementatie van de Privacy Richtlijn in de nationale wet. Er zijn dus ook verschillende toezichthoudende organen met afwijkende regelingen, verschillende sancties en boetes. Met de komst van de AVG zal men kennis maken met het “one-stop-shop” principe. Dit houdt in dat een internationale organisatie met vestigingen verspreid over verschillende lidstaten slechts onderworpen kan worden aan één toezichthouder. Deze “leidende toezichthouder” zal zich bevinden in de lidstaat waar de organisatie de hoofdzetel heeft.

Belangrijkste wijzigingen

De meeste regels onder de Wbp blijven na invoering van de AVG onverminderd van toepassing, aan het algemene doel van de regeling heeft de Europese wetgever niet willen tornen. Er zijn echter een aantal opvallende wijzigingen of aanscherpingen waar men als verantwoordelijke en als verwerker rekening mee dient te houden. Deze begrippen lichten wij toe.

Partijen waarop wetgeving van toepassing is

De Wbp kent een onderscheid tussen de verantwoordelijke of een derde die gegevens verwerkt, deze wordt onder de Wbp bewerker genoemd. Op grond van de AVG noemt men de verantwoordelijke ‘verwerkingsverantwoordelijke’ en de bewerker ‘verwerker’. De betrokkene is de persoon waarvan de persoonsgegevens verwerkt worden. Als de verwerkingsverantwoordelijke de verwerking door een derde-bewerker laat uitvoeren, gelden extra verplichtingen. De verwerkingsverantwoordelijke moet de bescherming van de persoonsgegevens van de betrokkene van derdeverwerker afdwingen door middel van een verplicht gestelde verwerkersovereenkomst. De Wbp gaat niet in op de precieze inhoud van de verwerkersovereenkomst maar geeft wel aan dat de verwerkingsverantwoordelijke in de overeenkomst moet bepalen hoever de verwerking gaat en welke middelen daarbij worden gebruikt. De verwerkingsverantwoordelijke moet ervoor zorgen dat de verwerker voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking. Ook moet de verwerkingsverantwoordelijke zorgen dat de bewerker de beveiligingsverplichtingen nakomt die op de verwerkingsverantwoordelijke rusten en dat uitsluitend voor de uitvoering van de opdracht de gegevens verwerkt worden.

De verplichtingen van de verwerkingsverantwoordelijke op grond van de Wbp, zijn onder de AVG nog steeds van toepassing. Waar de Wbp nog niet direct regels oplegt aan de verwerker, doet de AVG dit wel. Veel plichten welke aan de verwerkingsverantwoordelijke worden opgelegd, worden ook van toepassing verklaard op de verwerkers en ook krijgen zij aparte plichten zoals het feit dat zij aan de verantwoordelijke toestemming dienen te vragen voor sub-verwerking op grond van de wet. Overigens noemt men de bewerker op grond van de AVG “verwerker”. De verwerkersovereenkomst moet waarborgen dat er wordt voldaan aan het realiseren van passende technische en organisatorische

maatregelen zodat de verwerking aan de vereisten voldoet. Daarom worden in de AVG, in tegenstelling tot de Wbp, inhoudelijke eisen gesteld aan de verwerkersovereenkomst.

Wettelijke grondslagen voor gegevensverwerking
Op grond van de AVG gelden zes wettelijke grondslagen voor gegevensverwerking. Een belangrijke grondslag is dat de verwerking noodzakelijk kan zijn voor de uitvoering van een overeenkomst waarbij de betrokkene partij is. Een van de andere wettelijke grondslagen voor gegevensverwerking is gebaseerd op “toestemming van de betrokkene”. Op grond van de AVG zal deze wettelijke grondslag minder snel worden aangenomen, aangezien de uitleg hiervan is aangescherpt. In het geval van bijzondere persoonsgegevens, waarbij toestemming nodig is voor de verwerking, dient deze toestemming uitdrukkelijk te zijn. Dit was op grond van de Wbp nog niet het geval. In geval de betrokkene zijn toestemming geeft via een site kan dit worden bewerkstelligd door een vakje aan te klikken, een technische instelling of een andere duidelijke actie waaruit toestemming blijkt. Vooraf ingevulde/aangegeven toestemming op een site en het niet “weigeren hiervan” is geen toestemming meer op basis van de wet. Bedrijven die veel gebruik maken van dit soort impliciete toestemmingen kunnen dit na invoering van de AVG niet langer voortzetten.

DPIA (gegevensbeschermingseffectbeoordeling)
De meldplicht bij de AP in geval van geautomatiseerde gegevensverwerking van persoonsgegevens zal per 25 mei 2018 vervallen bij inwerkingtreding van de AVG. Hiervoor in de plaats komt de verplichting om voor risicovolle verwerkingen van persoonsgegevens een “Data Protection Impact Assessment” (DPIA) uit te voeren en daarbij in bepaalde gevallen de AP te raadplegen. Een DPIA is een instrument om privacy risico’s van een gegevensverwerking in kaart te brengen om vervolgens maatregelen te nemen om die risico’s te verkleinen. De DPIA bevat in ieder geval een beschrijving en het doel van de verwerking, evenals een beoordeling van de noodzaak en proportionaliteit van de verwerking, een inventarisatie van de betrokken risico’s, de bewaartermijn en de maatregelen die zullen worden getroffen om met deze risico’s om te gaan. Niet voor elke gegevensverwerking is een DPIA nodig, dit is alleen het geval als de verwerking waarschijnlijk een hoog privacy risico oplevert voor de betrokkenen. Dit kan in elk geval worden aangenomen indien bijvoorbeeld op grote schaal bijzondere persoonsgegevens worden verwerkt.

Meer handvatten zijn niet in de wet opgenomen over de verplichtstelling van de DPIA. De Europese privacy toezichthouders (WP 29) hebben in oktober 2017 de (definitieve) 'Guidelines on Data Protection Impact Assessment' gepubliceerd die meer uitleg geven over de DPIA. De AP gaat een lijst beschikbaar stellen van verwerkingen waarvoor een DPIA verplicht is.

Registerplicht en aangescherpte kwaliteitseisen
Naast de verplichting in bepaalde gevallen een DPIA uit te voeren, introduceert de AVG een documentatieplicht waarbij de verwerkingsverantwoordelijke wordt verplicht intern een register bij te houden van alle verwerkingsactiviteiten. Organisaties die minder dan 250 personen in dienst hebben worden van deze verplichting vrijgesteld, tenzij het waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen, de verwerking niet incidenteel is, of gevoelige persoonsgegevens bevat. Bij de AVG wordt meer nadruk gelegd op de verantwoordelijkheid

van organisaties zelf om de wet na te leven en om te kunnen aantonen dat zij zich aan de wet houden (accountability). De toezichthouder kan verzoeken om inzage van de administratie en schrijft in zijn algemeenheid voor dat een specifiek en modern beleid ontwikkeld dient te worden (gedragscodes, versleuteling en pseudonimisering) zodat kan worden beargumenteerd dat voldoende technische en organisatorische beveiligingsmaatregelen zijn genomen naar niveau van de wet. Het nadenken over risico's, waarborgen en gepaste beschermingsmaatregelen dient te gebeuren voorafgaand aan nieuwe projecten (privacy by design). Het beleid dient zodanig te zijn ingericht dat producten en diensten een standaard mate van gepaste gegevensbescherming in zich hebben, het systeem moet zo zijn ingesteld dat alleen persoonsgegevens worden verwerkt voor het specifieke doel dat de organisatie wil bereiken (privacy by default).

Functionaris voor de Gegevensbescherming (FG)
Een organisatie kan op grond van de Wbp besluiten een FG aan te stellen. Op basis van de Wbp is dit echtergeen verplichting. De AVG stelt dat bepaalde verantwoordelijken en verwerkers wel verplicht zijn een FG aan te stellen. Deze verplichting geldt bijvoorbeeld voor overheidsinstanties of publieke organen (uitgezonderd rechtbanken). De taken van een FG binnen een organisatie kunnen onder meer zijn: toezicht houden, inventarisatie van verschillende soorten gegevensverwerking, de meldingen van gegevensverwerking bijhouden, vragen en klachten van binnen en buiten de organisatie afhandelen, interne vaste regelingen ontwikkelen (compliance), adviseren over technologie en beveiliging (privacy by design) en input leveren bij het opstellen en aanpassen van een gedragscode. Deze vereisten en basistaken van de FG zijn onder de AVG vrijwel ongewijzigd gebleven. Aan de FG worden een aantal eisen gesteld:

1. Het moet gaan om een natuurlijk persoon;
2. De FG moet voldoende kennis hebben van de organisatie en de privacywetgeving;
3. De FG moet betrouwbaar zijn (geheimhoudingsplicht).

Bewaartermijnen: vage normen blijven gelden
Na inwerkingtreding van de AVG zal men niet ineens voor andere bewaartermijnen komen te staan. Het uitgangspunt blijft dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk is voor het doen van de verwerking. Hoe lang de gegevens bewaard mogen worden, verschilt aldus per geval. Wel dienen organisaties vooraf na te denken over het interne beleid omtrent het bewaren van gegevens. Men dient vast te leggen in het beleid hoe lang de gegevens bewaard moeten worden of welke criteria worden doorlopen om een bewaartermijn te bepalen. Het voorgaande kan worden vastgelegd in een bewaarbeleid. In het register van verwerkingen (indien verplicht) moeten de bewaartermijnen worden opgenomen. Op grond van de informatieverplichting moeten de betrokkenen worden geïnformeerd over de geldende termijnen. In geval van verwerking van persoonsgegevens voor het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden geldt een langere bewaartermijn. De gegevens mogen niet langer bewaard worden dan noodzakelijk is voor het oorspronkelijk doel.

Door dataminimalisatie (zo min mogelijk persoonsgegevens verwerken) en voornoemde doelbinding heeft de AVG wel invloed op de bewaartermijnen. In die zin, dat er beter over nagedacht dient te worden. Verklaard moet kunnen worden waarom een termijn wordt aangehouden, dat deze termijn zal worden vastgelegd en verstrekt aan de betrokkene.

Verder gelden natuurlijk nog altijd de bewaartermijnen op grond van specifieke wetten, bijvoorbeeld de werkgever die een kopie van ID-bewijs van een werknemer verwerkt (5 jaar, art. 66 lid 4 Uitvoeringsregeling LB).

Aangescherpte en aanvullende rechten betrokkenen

Op grond van de Wbp dienen organisaties welke persoonsgegevens verwerken een aantal belangrijke rechten van een betrokkene te respecteren en waarborgen. De bestaande rechten onder de Wbp blijven na invoering van de AVG overeind. De belangrijkste rechten zijn; het recht op informatie en transparantie, het inzagerecht, het rectificatierecht, recht van verzet, compensatie in geval van schade en toegang tot de nationale rechtsgang.

Het recht op informatie en transparantie zal na inwerkingtreding van de AVG worden uitgebreid. Verantwoordelijken zijn op grond van de AVG verplicht betrokkenen informatie te geven over de verwerking van hun persoonsgegevens. In duidelijke en eenvoudige taal dient een beknopt, transparant en toegankelijk rapport te worden afgegeven indien de betrokkene hierom vraagt. Vooral de hoeveelheid informatie die verstrekt moet worden, is in vergelijking met de Wbp groter. Die informatie betreft bijvoorbeeld: de periode waarvoor gegevens zullen worden opgeslagen, de rechten van betrokkene, de bron van de gegevens in geval deze niet rechtstreeks door betrokkene worden verstrekt en de juridische grondslag voor de verwerking van deze gegevens. De AVG heeft wel enige vorm van standaardisering in de toekomst goedgekeurd. Zij zal verwerkers voorzien van pictogrammen om de betrokkenen eenvoudig over de gegevensverwerking te informeren. Een set uitgebreide standaardinformatie zal waarschijnlijk voldoende zijn om in alle lidstaten aan de wettelijke informatieverplichting te voldoen.

Ook het correctierecht zal enigszins worden uitgebreid. De betrokkene kan eisen dat verwijdering van zijn gegevens zal geschieden bij alle organisaties die persoonsgegevens hebben verkregen van de verwerkingsverantwoordelijke (alle derden-verwerkers).

Twee nieuwe rechten zullen worden geïntroduceerd met de AVG. Het recht om vergeten te worden verplicht verwerkers van persoonsgegevens om op verzoek van betrokkene alle gegevens te wissen indien deze bij verdere verwerking inbreuk maken op de wet. Ook het recht van dataportabiliteit is nieuw. Dit zal inhouden dat in geval de betrokkene toestemming heeft gegeven voor de verwerking en zelf gegevens heeft aangeleverd, deze gegevens aan hem in een gestructureerd, gebruikelijk en leesbaar formaat moeten worden verstrekt als hij hier om vraagt. Op grond van de AVG moet de verantwoordelijke organisatie de betrokkene (soms op expliciete wijze) op deze rechten wijzen als hij de persoonsgegevens direct van de betrokkene verkrijgt. Het voorgaande zal waarschijnlijk een verzwaarde last worden voor organisaties, aangezien zij moeten bewerkstelligen dat de bestaande procedures voldoende zijn om alle rechten te waarborgen. Ook zullen nieuwe modellen moeten worden gemaakt om aan het recht van dataportabiliteit te kunnen voldoen.

Meldplicht datalekken

In Nederland geldt vanaf 1 januari 2016 de wettelijke verplichting om datalekken te melden; deze is opgenomen in de Wbp. Deze meldplicht houdt in dat verantwoordelijke organisaties onverwijld een melding moeten doen bij de AP zodra zij een ernstig datalek ontdekken. In een aantal gevallen moeten

organisaties het datalek ook melden aan de betrokkenen. Met de komst van de AVG zijn niet veel inhoudelijke wijzigingen aangebracht. De hoofdregels gelden nog steeds, met enkele nuanceverschillen. Wel van belang is dat de AVG een systeem van verplichte melding voor datalekken voor alle EU-lidstaten introduceert. Onder de AVG moet een overzicht worden bijgehouden van ALLE inbreuken op de beveiliging, terwijl dit nu alleen bij meldingsplichtige inbreuken geldt.

Slotopmerking

Het is van groot belang dat men zich als organisatie bewust is van de nieuwe wetgeving omtrent de verwerking van persoonsgegevens. Vóór 25 mei 2018 dienen organisaties alle mogelijke veranderingen welke de AVG binnen deze organisaties teweeg brengen te hebben geïmplementeerd.