Mr. S. Bastiaans[1]

Privacy in een nieuw jasje: een vergelijking van beschermingsniveau tussen de Wbp en de AVG

Bb 2018/24

De AVG zal op 25 mei 2018 inwerking treden. Dit zal de privacyregelgeving aanscherpen. Door een territoriale uitbreiding van het toepassingsbereik van de regelgeving, meer focus te leggen op (verplichte) controle van naleving van de verordening voorafgaand aan een verwerking van persoonsgegevens, in combinatie met een uitgebreider arsenaal aan handhavingsinstrumenten voor de Autoriteit Persoonsgegevens, zal de bescherming van privacy voor burgers in de EU toenemen.

1. Inleiding

Op 25 mei 2018 zal de Algemene verordening gegevensbescherming (hierna: AVG) inwerking treden in de gehele Europese Unie (hierna: EU). Hiermee worden de Privacyrichtlijn (95/46/EG) en de Nederlandse implementatie daarvan, de Wet bescherming persoonsgegevens (hierna: Wbp), ingetrokken. Dit brengt een aantal wijzigingen met zich mee, die de privacy van burgers ten goede moet komen. In deze bijdrage zullen de wet en de verordening naast elkaar gelegd worden en zal beoordeeld worden in hoeverre de AVG daadwerkelijk een stap vooruit betreft in de bescherming van privacy van burgers. Allereerst zal het materiële en territoriale toepassingsgebied van beide regelgevingen uiteengezet worden (paragraaf 2). Vervolgens zullen de verplichtingen voor verwerkingsverantwoordelijken (paragraaf 3) en de rechten van betrokkenen (paragraaf 4), volgend uit de Wbp en de AVG, gepresenteerd worden en zal in paragraaf 5 de vergelijking betreffende toezicht en de handhaving centraal staan. Afgesloten wordt met een conclusie (paragraaf 6), waaruit zal blijken of de AVG daadwerkelijk het niveau van privacy bij gegevensverwerking van burgers omhoog brengt.

2. Het toepassingsbereik van privacyregelgeving

2.1 *Het materiële toepassingsbereik*

Het materiële toepassingsbereik van de AVG is ten opzichte van de Wbp nauwelijks gewijzigd. De AVG is ex art. 2, eerste lid, AVG van toepassing op de geheel of gedeeltelijke geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Dit is volledig in lijn met het toepassingsbereik van de Wbp (art. 2, eerste lid, Wbp). Ook de definitie van "persoonsgegevens" is, ondanks enkele ingediende maar verworpen amendementen, nauwelijks gewijzigd. Het betreft krachtens art. 4, eerste lid, AVG 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon'. De wijze waarop een natuurlijk persoon direct of indirect (lees: zonder oneven-redige inspanning) geïdentificeerd kan worden, is onder het regime van de AVG ten opzichte van de Wbp uitgebreid, of gemoderniseerd. Zo worden nu expliciet de online identificator, zoals *cookies* en IP-adressen, en locatiegegevens als persoonsgegevens genoemd.

2.2 *Het territoriale toepassingsbereik*

De vergelijking tussen beide vormen van regelgeving wordt interessanter bij het territoriale toepassingsbereik. Daar waar de Wbp ex art. 4 Wbp van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland en op verantwoordelijken die buiten de EU zijn gevestigd, maar bij de verwerking gebruik maken van middelen die zich in Nederland bevinden (tenzij de middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens), betreft dit 'gebruik van techniek' voor de verwerking van persoonsgegevens onder de AVG niet langer het enige aanknopingspunt voor het toepasselijke recht. De AVG is ex art. 3, eerste lid, AVG van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie al dan niet plaatsvindt. Een belangrijke uitbreiding op het territoriale toepassingsbereik van de Europese privacyregelgeving betreft echter art. 3, tweede lid, AVG. De verordening is namelijk eveneens van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich in de Unie bevinden, door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker, indien de verwerking verband houdt met het aanbieden van goederen of diensten aan deze betrokkenen. Dus ook zónder vestiging in de EU en zónder het gebruikmaken van technieken die zich wel in de EU bevinden, genieten EU-burgers bescherming van hun privacy door de AVG indien een verwerking ziet op het aanbieden van goederen of diensten aan hen. Dit betekent dat IT-giganten als Google, Facebook en Amazon, die allen persoonsgegevens van burgers in de EU verwerken ter aanbieding van hun goederen of diensten, nu hoe dan ook rechtstreeks onder het EU privacy regime gaan vallen.

3. Verplichtingen voor verwerkingsverantwoordelijken

3.1 *Voorwaarden voor rechtmatige verwerking*

Persoonsgegevens mogen onder het oude en nieuwe privacyrecht slechts op een behoorlijke en zorgvuldige wijze worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (vgl. art. 6 jo. 7 Wbp met art. 5 jo. 6 AVG). Nieuw is dat overheidsinstanties niet langer een verwerking louter mogen baseren op het doel 'gerechtvaardigd belang' (art. 6, eerste lid, onder f, AVG) en

1 Steven Bastiaans is advocaat bij Stibbe te Amsterdam.

dat er voor overheidsinstanties, wegens de wanverhouding tussen de betrokkene en de verwerkingsverantwoordelijke, aanvullende eisen worden gesteld aan 'toestemming' als rechtvaardigingsgrond. De gegeven toestemming zal bij sommige verwerkingen namelijk uit noodzaak niet geheel vrijelijk zijn verleend (zie overweging 43 AVG). Overigens vervalt de verplichting ex art. 27 Wbp tot het melden van een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens bij de Autoriteit Persoonsgegevens (hierna: AP) onder het regime van de AVG. Meer dan voorheen moeten verwerkers nu zelf verantwoording kunnen afleggen over hun dataverwerkingen, door zelf een register bij de houden; de zogeheten "*accountability*".

3.2 ***De functionaris voor de gegevensbescherming***

De Wbp kende reeds in art. 62 Wbp de mogelijkheid voor een verantwoordelijke tot het instellen van een functionaris voor de gegevensbescherming (hierna: FG). Een FG informeert en adviseert onafhankelijk verantwoordelijken over hun verplichtingen bij het realiseren van de naleving van privacyregelgeving. Het instellen van een FG was echter volledig facultatief. Dit verandert onder de AVG. Hoewel de Europese Commissie in haar ontwerpverordening van de AVG de FG nog verplicht wilde stellen voor elke overheidsinstantie en elk particulier bedrijf met meer dan 250 werknemers, rust deze verplichting in de definitieve tekst van art. 37, eerste lid, AVG slechts op overheidsinstanties en verantwoordelijken die belast zijn met grootschalige verwerkingen van bijzondere categorieën van persoonsgegevens. Het zal nog moeten blijken of een FG daadwerkelijk volledig onafhankelijk zijn taak kritisch kan vervullen binnen deze instanties.

3.3 ***DPIA, 'privacy by design' en 'privacy by default'***

Verder introduceert de AVG enkele begrippen voor verwerkingen die reeds onder het regime van de Wbp in het ongeschreven recht bestonden, maar nu voor het eerst gecodificeerd zijn. Dit betreft de *Data Protection Impact Assessment* (hierna: DPIA), het bij sommige verwerkingen verplicht uitvoeren van een risicoanalyse en, waar nodig, preventief ingrijpen om een foutieve omgang met persoonsgegevens te voorkomen (art. 35 e.v. AVG) en het begrippenpaar *'privacy by design'* en *'privacy by default'* (art. 25 AVG). 'Privacy by design' vereist dat reeds bij het bepalen van de te gebruiken verwerkingsmiddelen, zoals ICT-systemen, rekening dient te worden gehouden met de principes en verplichtingen uit de AVG. 'Privacy by default' vereist dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke te bereiken verwerkingsdoel. Er zitten hiermee onder meer restricties op de hoeveelheid te verzamelen gegevens en de termijn waarvoor zij worden opgeslagen (zie art. 25, tweede lid, AVG).

3.4 ***Meldplicht datalekken***

Nederland heeft een voorschot genomen op de notificatieplicht bij datalekken uit art. 33 jo. 34 AVG door de invoer van de Wet meldingsplicht datalekken in 2016. Als er een datalek heeft plaatsgevonden, dient de verantwoordelijke dit in beginsel binnen 72 uur na bekendheid met het lek aan de toezichthouder te melden. Daar waar onder de Wbp slechts 'ernstige' lekken gemeld dienen te worden (art. 34a Wbp), moet er onder de AVG in beginsel elk lek worden gemeld tenzij niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen (positieve verplichting). Op de niet-naleving van deze verplichting staan hoge boetes.

4. Rechten voor betrokkenen

4.1 ***Inzage, rectificatie en right to be forgotten***

Betrokkenen hebben zowel onder de Wbp als onder de AVG het recht op inzage van hem betreffende persoonsgegevens (vgl. art. 35 Wbp met art. 15 AVG) en, indien blijkt dat de verwerker onjuiste of onvolledige persoonsgegevens hanteert, het recht tot rectificatie van deze gegevens (vgl. art. 36 Wbp met art. 16 AVG). Betrokkenen kennen onder de Wbp tevens het "recht tot vergetelheid", waarbij zij kunnen verzoeken om zonder onredelijke vertraging persoonsgegevens door een verantwoordelijke te laten wissen. Daar waar dit nu nog volgt uit het arrest *Google Spain* (HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317), is het *right to be forgotten* onder de AVG voor het eerst gecodificeerd (art. 17 AVG), waardoor het mogelijk meer toepassing zal genieten.

4.2 ***Recht op dataportabiliteit***

Nieuw in de AVG is het recht op dataportabiliteit, of het recht op gegevensoverdraagbaarheid. Een betrokkene die zijn persoonsgegevens zelf aan een verantwoordelijke verstrekt, krijgt ex art. 20, eerste lid, AVG het recht om teruggave van deze gegevens te verlangen om deze aan een andere verantwoordelijke over te dragen. Dit moet het zelfbeschikkingsrecht vergroten. Denk hierbij aan het behoud van een gsm-nummer na wisseling van provider. Een voorwaarde hierbij is dat uitwisseling van de gegevens technisch mogelijk is, zie art. 20, tweede lid. AVG.

5. Toezicht en handhaving

5.1 ***Nationale toezichthouder en haar taken***

Nederland heeft onder de Wbp (art. 51 Wbp) en onder de AVG (art. 51 AVG) een onafhankelijke nationale toezichthouder ingesteld, de Autoriteit Persoonsgegevens. Dit orgaan is belast met het toezicht op de naleving van privacywetgeving, teneinde de grondrechten en vrijheden van natuurlijke personen in verband met de verwerking van hun persoonsgegevens te beschermen. Daar waar de taak van de AP onder de Wbp slechts bestond uit toezichthouden en handhaven (art. 51 e.v. Wbp), heeft deze onder de AVG ook een expliciete informerende en adviserende rol (art. 57 AVG).

5.2 ***Sanctionering***

De Wbp kent verschillende handhavingsinstrumenten, zoals een last onder bestuursdwang (art. 65 Wbp), een bestuurlijke boete (art. 66 Wbp) en een strafrechtelijke geldboete (art. 75 Wbp). Daarnaast kan de AP een onderzoek

instellen naar de wijze waarop gegevens worden verwerkt (art. 60 Wbp) en een woning betreden zonder toestemming van de bewoner (art. 61, tweede lid, Wbp). De AVG vergroot en verzwaart het arsenaal aan bevoegdheden van de AP. De corrigerende maatregelen die de AP kan nemen volgen uit art. 58 AVG. Zo kan de AP, naast de handhavingsinstrumenten die zij reeds onder de Wbp bezat, nu ook berispen of een tijdelijk of definitief verwerkingsbeperking, waaronder zelfs een algeheel verwerkingsverbod, opleggen. De hoogte van de door de AP maximaal op te leggen geldboete is onder de AVG aanzienlijk gestegen (art. 83, vierde en vijfde lid. AVG). Daar waar de maximumboete onder de Wbp (ná 1 januari 2016) € 20.250 respectievelijk € 810.000 bedraagt, afhankelijk van de overtreding, zal dit onder de AVG € 10.000.000 (of 2% van de totale wereldwijze jaaromzet) of € 20.000.000 (of 4% van de totale wereldwijde jaaromzet) zijn, afhankelijk van de overtreding.

6. Conclusie

De AVG werd door sommigen aangekondigd als de belangrijkste wetgeving van de 21e eeuw. Hoewel er enkele praktische valkuilen open blijven, betekent de AVG ten opzichte van de Wbp wel degelijk onderaan de streep een stap vooruit wat betreft de bescherming van burgers bij gegevensverwerking. Vooral de uitbreiding van het territoriale toepassingsbereik, de verplichting tot accountability van verwerkingen, de codificering van de DPIA, het recht op vergetelheid en de beginselen 'privacy by design' en 'privacy by default', het afschrikwekkende effect dat de torenhoge maximumboetes bij niet-naleving van de privacyregels met zich meebrengen en de voor overheden verplichte aanstelling van een FG zullen het beschermingsniveau positief beinvloeden. Het betreft weliswaar een kleinere stap dan door sommigen werd gehoopt, maar bij een gewichtig belang als dat van privacy van burgers, is elke stap goud waard.