

Vergaderjaar 2022–2023

32 761

Verwerking en bescherming persoonsgegevens

Nr. 284

BRIEF VAN DE MINISTER VOOR RECHTSBESCHERMING

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 18 september 2023

Op 6 september 2022 heb ik het onderzoeksrapport «Bescherming gegeven? Evaluatie UAVG, meldplicht datalekken en de boetebevoegdheid» aan uw Kamer aangeboden dat in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) is uitgevoerd door Pro Facto en Hooghiemstra & Partners (Kamerstuk 32 761, nr. 246). Met deze brief ontvangt u, mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties, de beleidsreactie op dat onderzoek, nadat de context van het onderzoek is toegelicht.

Context

De Algemene Verordening Persoonsgegevens (AVG) is rechtstreeks van toepassing in Nederland. Op 25 mei 2018 is de Uitvoeringswet Algemene verordening persoonsgegevens (UAVG) in werking getreden. Deze wet vult voor Nederland voor een belangrijk deel de ruimte in die de Europese lidstaten op grond van de AVG hebben om op bepaalde punten meer specifieke nationale regelingen te treffen. Daarnaast geeft de UAVG invulling aan de verplichting uit de AVG om in elke lidstaat een onafhankelijke autoriteit verantwoordelijk te maken voor het toezicht op de toepassing van de verordening. Voor Nederland is dat de Autoriteit Persoonsgegevens (AP).

Bij de totstandkoming van de UAVG heeft de wetgever ervoor gekozen om, los van de veranderingen die de AVG met zich meebrengt, de nationale keuzes zoveel mogelijk beleidsneutraal door te voeren. Dat wil zeggen dat is aangesloten bij de toen geldende Wet bescherming persoonsgegevens (Wbp). Hier is voor gekozen om de invoering van de AVG zo vloeiend mogelijk te laten verlopen ten opzichte van de bestaande situatie; de inwerkingtreding van de AVG zorgde immers al voor grote veranderingen.

Artikel 50 van de UAVG bepaalt dat binnen drie jaar na inwerkingtreding van de wet verslag zal worden gedaan van de effecten van de wet in de

praktijk en van de uitvoering van de wet in de praktijk. Het onderhavige onderzoek behelst een evaluatie van de UAVG en geeft zodoende uitvoering aan de evaluatiebepaling in de wet. De evaluatie van de UAVG is bedoeld om inzicht te bieden in de vraag in hoeverre de bepalingen in de UAVG helder, toegankelijk, uitvoerbaar en handhaafbaar zijn. Daarnaast dient de evaluatie om de uitvoering van de wet in de praktijk in kaart te brengen.

Het onderhavige onderzoek heeft eveneens aandacht besteed aan de motie van de Kamerleden Schouw en Segers uit 2015 waarin de regering wordt verzocht de Wet meldplicht datalekken en boetebevoegdheid binnen vier jaar na inwerkingtreding te evalueren.¹ De Wet meldplicht datalekken en boetebevoegdheid is weliswaar komen te vervallen met de inwerkingtreding van de AVG, maar de naleving van de (nu in de AVG opgenomen) meldplicht en de toepassing en de effectiviteit van de boetebevoegdheid zijn onverminderd relevant. Binnen de evaluatie van de UAVG is om die reden onderzocht hoe de meldplicht datalekken wordt nageleefd en in hoeverre de boetebevoegdheid van de AP bijdraagt aan de doelmatige en doeltreffende uitvoering en handhaving van de UAVG.

Hoewel de UAVG moeilijk los te zien is van de AVG, betreft dit onderzoek expliciet *geen* evaluatie van de AVG. De AVG zelf wordt door de Europese Commissie geëvalueerd; op 24 juni 2020 heeft zij het eerste evaluatieverslag van de AVG gepubliceerd.² Evenmin heeft het onderzoek zich gericht op de onderdelen in de UAVG die fungeren als instellingswet van de AP.

Het onderzoek bestaat als gezegd uit twee delen: de evaluatie van de UAVG zelf en de uitvoering van het verzoek dat uw Kamer heeft gedaan bij motie van de toenmalige Kamerleden Schouw en Segers uit 2015, waarin de regering wordt verzocht de Wet meldplicht datalekken en boetebevoegdheid binnen vier jaar na inwerkingtreding te evalueren. In het eerste deel van deze reactie wordt ingegaan op de wetsevaluatie en in het tweede deel op de uitwerking van de motie.

Onderdeel 1: Evaluatie van de UAVG

1. Algemeen

Door de beleidsneutrale omzetting van de bestaande normen onder de Wbp is volgens de onderzoekers de toegevoegde waarde van de UAVG beperkt. De normen uit de AVG zijn open geformuleerd, wat maakt dat zij uitleg per concreet geval behoeven voordat ze handhaafbaar zijn. In de UAVG is de mogelijkheid van een meer specifieke invulling en concretisering volgens de onderzoekers niet voldoende benut. Die nadere invulling is er volgens de onderzoekers evenmin gekomen in de jurisprudentie, nu het aantal gepubliceerde uitspraken waarin de UAVG een materiële rol speelt, beperkt is.

Het is juist dat bij de totstandkoming van de UAVG de bewuste keuze is gemaakt om grotendeels aan te sluiten bij de bestaande privacyreggeving, enerzijds vanwege het korte tijdsplan voor de implementatie en anderzijds om de overgang naar de AVG zo soepel mogelijk te laten verlopen. Dat maakt naar mijn oordeel echter niet dat de waarde van de UAVG beperkt is. Allereerst kent de UAVG wel degelijk nadere invullingen, bijvoorbeeld waar het gaat om uitzonderingen op het verwerkingsverbod van bijzondere persoonsgegevens en gegevens van strafrechtelijke aard.

¹ Kamerstuk 33 662, nr. 20.

² Kamerstukken 22 112 en 32 761, nr. 2994.

Belangrijker is misschien wel dat de UAVG niet gezien moet worden als de enige nationale wet die uitvoering geeft aan de AVG. Dat gebeurt ook ruimschoots in sectorale wetgeving, waarin het vaak beter mogelijk is op de specifieke materie toegesneden normen te stellen dan in een algemene wet als de UAVG. Deze systematiek strookt ook met de aanbeveling die de onderzoekers doen om zoveel mogelijk in sectorwetgeving te regelen en slechts algemene, sectoroverstijgende zaken in de UAVG te regelen. Voor dat laatste is het, juist nu het gaat om open normen, belangrijk dat de flexibiliteit behouden blijft om de rechtsontwikkeling ervan grotendeels in de praktijk te laten plaatsvinden.

Dat neemt uiteraard niet weg dat op gezette tijden bezien moet worden of de wetgeving aanpassing behoeft. Dat is ook de afgelopen jaren gebeurd, met als resultaat dat op 2 december 2022 de Verzamelwet gegevensbescherming is ingediend bij uw Kamer. In dit wetsvoorstel wordt een aantal wijzigingsvoorstellen gedaan, niet alleen van de UAVG maar ook van diverse andere wetten. Enkele aanbevelingen die gedaan worden door de onderzoekers in het kader van de onderhavige evaluatie, zijn daarin reeds ondervangen. Eventuele verdere wijzigingen zullen in toekomstige wets(wijzigings)trajecten worden meegenomen. Dat geldt ook ten aanzien van de voorstellen die de Autoriteit Persoonsgegevens heeft gedaan in haar brief van 23 januari 2023, houdende aanvullende thema's ter overweging bij de evaluatie UAVG en een volgende wetswijziging. Op deze wijze kan het lopende wetsvoorstel Verzamelwet verder worden behandeld. Een ingrijpende uitbreiding van dat wetsvoorstel in dit stadium zou betekenen dat het opnieuw aan de AP en de Afdeling Advisering van de Raad van State zou moeten worden voorgelegd, wat leidt tot aanzienlijke vertraging voor de wijzigingen die daarin reeds voorgesteld worden.

2. Gedragscodes

Om meer eenduidigheid te brengen in de toepassing van de bepalingen uit de AVG, zien de onderzoekers niet alleen een rol voor de toezichthouder, maar ook voor sectoren en organisaties zelf. Een belangrijk instrument daarbij is de gedragscode. In de praktijk wordt, zo blijkt uit het onderzoek, het opstellen van een gedragscode gezien als een proces dat veel energie kost en waarvan het onzeker is of de eindstreep van de goedkeuring wordt gehaald. De animo om een gedragscode ter goedkeuring aan de AP voor te leggen lijkt laag te zijn, mede omdat te weinig duidelijk is aan welk normenkader de toezichthouder toetst. Om de totstandkoming van het aantal gedragscodes en het vragen van de goedkeuring daarvan te laten toenemen, kan het volgens de onderzoekers behulpzaam zijn om in sectorale wetgeving het hebben van een goedgekeurde gedragscode te verplichten. Op deze wijze worden sectoren gedwongen om tot zelfregulering te komen.

In het commissiedebat van 22 november 2022 inzake de verwerking en bescherming van persoonsgegevens heb ik, op een vraag van het Kamerlid Van Ginneken (D66), toegezegd schriftelijk te zullen ingaan op de mogelijkheden om gedragscodes te bevorderen.³ Met deze brief voldoe ik tevens aan deze toezegging. Het betreft hier een aandachtspunt dat in de gehele Unie speelt. Het kader voor gedragscodes is grotendeels neergelegd in de AVG zelf, daarom zijn de mogelijkheden beperkt om de UAVG hiervoor aan te passen. Zoals de onderzoekers al vaststellen, zal de ontwikkeling van dit instrument in belangrijke mate op de weg liggen van de verwerkingsverantwoordelijken, de nationale toezichthouder, de European Data Protection Board (EDPB) en uiteindelijk de rechter. Ik ben

³ Kamerstuk 32 761 nr. 249.

geen voorstander van het verplicht stellen in sectorale wetgeving van het hebben van een goedgekeurde gedragscode. Een gedragscode is naar zijn aard een instrument dat opgesteld moet worden door een sector zelf en draagvlak moet hebben binnen een sector, wil het een goede werking hebben. Het kent een zekere mate van vrijwilligheid om er aansluiting bij te zoeken. Wel zal ik in overleg treden met de AP over de mogelijkheden die bestaan voor het verder brengen van dit instrument en het belang daarvan onder de aandacht brengen.

3. De naleving van de normen

Ten aanzien van de naleving van de bepalingen in de UAVG merken de onderzoekers op dat sprake is van een nog voortgaand proces van bewustwording en implementatie binnen organisaties. Er is intussen steeds meer aandacht voor de bescherming van persoonsgegevens, maar is er ook nog ruimte voor verbetering. Deze observatie deel ik. Er is sinds de inwerkingtreding van de AVG en de UAVG een veel groter privacy-bewustzijn ontstaan, niet alleen in Nederland, maar in heel Europa en zelfs daarbuiten. Uit het WODC-onderzoek «Verkennde analyse: Naleving van de AVG door overheden», dat ik op 25 januari 2023 aan uw Kamer heb aangeboden, komt ook naar voren dat aandacht voor een correcte verwerking van persoonsgegevens na invoering van de AVG een positieve ontwikkeling heeft doorgemaakt en dat de kennis van het gegevensbeschermingsrecht toeneemt.

De constatering van de onderzoekers in de evaluatie dat de UAVG niet altijd even bekend is en dat niet altijd gerefereerd wordt aan de UAVG door bijvoorbeeld rechters, is op zichzelf niet problematisch. Het gaat erom dat het gegevensbeschermingsrecht – dat in belangrijke mate Unierechtelijke begrippen kent – als geheel wordt nageleefd. Hieronder wordt ingegaan op de specifieke aanbevelingen in het onderzoek.

4. Aanbevelingen

Biometrische gegevens

De onderzoekers merken op dat de uitzonderingsgrond voor de verwerking van biometrische gegevens op dit moment onvoldoende duidelijk is. In het conceptvoorstel voor de Verzamelwet gegevensbescherming wordt artikel 29 UAVG nader aangescherpt en verduidelijkt. Aan de aanbeveling over deze bepaling is voldaan door in toelichting bij dit artikel (onderdeel K) een reeks aanvullende voorbeelden te geven van een zwaarwegend algemeen belang. In het verslag bij de Verzamelwet zijn hierover verdere vragen over gesteld, waarop nader ingegaan zal worden in de nota naar aanleiding van het verslag.⁴

Cross-sectorale gegevensdeling

Onder de UAVG is het mogelijk om persoonsgegevens van strafrechtelijke aard ten behoeve van derden te verwerken, onder andere indien de AP hiervoor een vergunning heeft verleend. De AP kan een dergelijke vergunning verlenen, indien de verwerking noodzakelijk is met het oog op een zwaarwegend belang van derden en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Tot vergunningverlening ten aanzien van het cross-sectoraal delen van gegevens is de AP vooralsnog niet overgegaan, omdat naar haar oordeel tot nu toe geen aanvraag voldeed aan de voorwaarden (kort gezegd: noodzakelijke verwerking, zwaar-

⁴ Kamerstuk 36 264, nr. 5.

wegend belang van derden en voldoende waarborgen). De onderzoekers werpen de vraag op of binnen de huidige systematiek – door middel van vergunningverlening door de toezichthouder – cross-sectorale gegevensdeling door private partijen wel gerealiseerd kan worden. In het geval er een politieke wens ligt om cross-sectorale gegevensdeling tussen private partijen mogelijk te maken, dan zou het meer voor de hand liggen om dit in afzonderlijke wetgeving met de nodige waarborgen omkleed te regelen, zo stellen de onderzoekers. Indien het cross-sectoraal delen van gegevens *niet* wenselijk wordt geacht, dan zou de UAVG op dit punt aan duidelijkheid kunnen winnen door deze wijze van delen van persoonsgegevens expliciet in artikel 33 van vergunningverlening uit te sluiten, aldus de onderzoekers.

Naar mijn oordeel is het te vroeg om gevolg te geven aan deze suggestie. Dat de AP de twee tot op heden geweigerde aanvragen ontoereikend vond in het licht van de gestelde eisen, wil niet zeggen dat het nu al duidelijk is dat het vergunningenstelsel uit artikel 33, vierde lid UAVG niet in stand moet blijven. In dit verband staat nog overeind de mededeling aan uw Kamer van het vorige kabinet in 2019⁵ dat de ervaringen worden afgewacht die door private organisaties worden opgedaan met hun voornemen tot cross-sectorale gegevensdeling, en dat afhankelijk van die ervaringen zo nodig nieuwe wetgeving zal kunnen worden overwogen. Op 15 juli 2021 heeft de AP een «Handreiking cross-sectorale gegevensdeling tussen private partijen» gepubliceerd. Het is inderdaad – zoals de onderzoekers ook opmerken – zo dat het cross-sectoraal delen tussen private partijen van de hier bedoelde gegevens niet is toegestaan, tenzij wordt voldaan aan zeer hoge eisen. Die eisen vloeien voort uit de AVG en in mindere mate uit de UAVG. Dat betekent dat ook wanneer cross-sectorale gegevensdeling in afzonderlijke wetgeving zou worden geregeld, de in die wetgeving op te nemen voorwaarden net als nu gebonden zullen zijn aan de minimale vereisten van de AVG. Deze vorm van uitwisseling zal dus ook dan alleen in zeer uitzonderlijke gevallen zijn toegestaan omdat deze eisen ertoe leiden dat vooral vergunningen voor sectorale gegevensdeling of gegevensdeling met een beperkte reikwijdte worden verleend. Met deze eisen van de AVG zal bij een eventuele wetswijziging ook rekening moeten worden gehouden, hetgeen maakt dat de materiele meerwaarde van wetswijziging beperkt zal zijn. Dat voor het cross-sectoraal delen van persoonsgegevens noodzakelijkheid, subsidiariteit en proportionaliteit goed onderbouwd moeten worden, zal te allen tijde vereist zijn, zowel bij een vergunningensystematiek, als in het geval er wetgeving zou worden opgesteld. Er zal altijd duidelijk moeten zijn wat het doel en de noodzaak is van het cross-sectoraal delen van persoonsgegevens van strafrechtelijke aard, welke gegevens dan precies mogen worden verwerkt en vooral ook wat de waarborgen zijn voor de betrokkenen. Het gaat immers om gevoelige gegevens, waarmee zeer zorgvuldig moet worden omgegaan, omdat de gevolgen van verwerking ervan voor betrokkenen zeer verstrekkend kunnen zijn. Op dit moment wordt met publieke en private partijen de noodzaak van gegevensdeling ten behoeve van criminaliteitsbestrijding in kaart gebracht.⁶ Uit de verkenning zoals is aangekondigd in het actieprogramma online fraude komt naar voren dat het gebrek aan mogelijkheden voor gegevensdeling een belemmering is voor een effectieve aanpak. Er zal worden bezien of en zo ja hoe deze belemmeringen kunnen worden weggenomen. De resultaten van de verkenning zal de Minister van Justitie en Veiligheid zo spoedig mogelijk met uw Kamer delen.

⁵ Kamerstuk 32 761, nr. 151, p. 10.

⁶ Kamerstuk 29 911, nr. 393 en bijlage.

Rechtsbescherming

De onderzoekers doen enkele aanbevelingen op het terrein van de rechtsbescherming tegen niet-naleving van de AVG en de UAVG, zowel op bestuursrechtelijk als civielrechtelijk terrein. Ook gaan zij in op rechtsbescherming bij geautomatiseerde besluitvorming.

Het onderzoek beschrijft allereerst in welke gevallen kan worden opgekomen tegen besluiten die zien op een verzoek van een betrokkene over de uitoefening van zijn rechten uit hoofde van artikel 15 tot en met 22 AVG. Als de verwerkingsverantwoordelijke een bestuursorgaan is, dan is volgens het onderzoek de effectiviteit van de rechtsbescherming op grond van artikel 34 UAVG beperkt, omdat daarin niet wordt voorzien in rechtsbescherming tegen feitelijke bestuurshandelingen (niet zijnde besluiten). Er wordt geadviseerd om in ieder geval, in navolging van uitspraken van de Afdeling bestuursrechtspraak van de Raad van State,⁷ onrechtmatig handelen door middel van een onrechtmatige gegevensverwerking los te kunnen beoordelen van een daaropvolgend (onrechtmatig) besluit. De onderzoekers geven in overweging de mogelijkheid te creëren om vroegtijdig, dus zonder dat er al een besluit in de zin van artikel 1:3, eerste lid Awb moet zijn genomen, de juistheid van een verwerking te betwisten. Zo zou in de UAVG een bepaling kunnen worden opgenomen die in afwijking van artikel 8:88, eerste lid, aanhef en onder b Awb beroep bij de bestuursrechter openstelt voor degene die op grond van artikel 82 AVG aanspraak stelt te maken op vergoeding van schade die het gevolg is van het onrechtmatig verwerken van persoonsgegevens en daarmee het onrechtmatig bestuurlijke handelen door een bestuursorgaan zonder dat reeds een (onrechtmatig) besluit door dat bestuursorgaan is genomen.

Mijn ambtsvoorganger heeft in het commissiedebat van 20 mei 2020⁸ inzake de verwerking en bescherming van persoonsgegevens toegezegd dat er schriftelijk ingegaan zou worden op de mogelijkheden van meer gegevensbescherming in het bestuursrecht.⁹ Ik heb oog voor de onderliggende problematiek dat er sprake kan zijn van onrechtmatige gegevensverwerking door de overheid, zonder dat er ook al sprake is van een (onrechtmatig) besluit. De rechtsontwikkeling op dit punt volg ik dan ook met belangstelling. Vooralsnog lijkt de rechtspraak binnen de bestaande kaders te beschikken over voldoende mogelijkheden om tot een beoordeling te komen ten aanzien van voorbereidende feitelijke handelingen. De in het onderzoek aangehaalde jurisprudentie van de Afdeling bestuursrechtspraak van de Raad van State geeft immers belangrijke nuanceringen ten aanzien van het gegevensbeschermingsrecht. De gevolgen daarvan voor de praktijk zullen zich de komende tijd aftekenen. Indien daaruit een breder gedragen wens naar voren komt dat het wettelijk kader herziening behoeft, dan kan daar tegen die tijd met inachtneming van de uitspraken van de hoogste bestuursrechter naar worden gehandeld. Met vorenstaande ga ik ook in op voormelde toezegging.

Verder hebben de onderzoekers zich uitgesproken over de effectiviteit van de civiele rechtsbescherming, ofwel de rechtsbescherming ten opzichte van niet-overheidsorganen. Die kent nu twee procedures: de verzoekschriftprocedure (die gerelateerd is aan een verzoek als bedoeld in de

⁷ ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, *JBP* 2020/56 en ABRvS 22 februari 2022, ECLI:NL:RVS:2022:319.

⁸ Kamerstuk 32 761, nr. 192.

⁹ Daarbij was onder meer aan de orde een artikel van Fatma Capkurt uit het Nederlands Tijdschrift voor Bestuursrecht (NTB 2021/61). In dit artikel wordt betoogd dat het bestuursrechtelijke besluitbegrip anders zou moeten worden geïnterpreteerd, opdat persoonsgegevensverwerkingen die een bestuursorgaan verricht en die nauw verbonden zijn met een besluit onder de reikwijdte van dat begrip komen te vallen.

artikelen 15 tot en met 22 AVG) en de dagvaardingsprocedure (voor alle aanvullende aangelegenheden). De onderzoekers bevelen ook aan om de verzoekschriftprocedure uit te breiden. Nu kent deze procedure slechts de mogelijkheid om een verzoek als bedoeld in artikel 15 tot en met 22 AVG toe of af te wijzen, maar de onderzoekers stellen voor om onderdeel van de procedure te maken het eventuele ongedaan maken van de onrechtmatige verwerking alsmede de mogelijkheid om schadevergoeding te verzoeken. Met deze uitbreidingen zouden betrokkenen niet langer de complexere dagvaardingsprocedure hoeven te starten. Ik vind de gedachte om de rechtsbescherming voor betrokkenen laagdrempeliger te maken het onderzoeken waard. Daartoe moet niet alleen in kaart worden gebracht in hoeverre deze behoefte in de praktijk bestaat, maar ook wat de consequenties zullen zijn van opvolging van het voorstel van de onderzoekers, bijvoorbeeld in aantallen verzoekschriftprocedures bij de rechtbanken. Uw Kamer wordt hierover op een later moment nader geïnformeerd.

De onderzoekers hebben verder uit jurisprudentieonderzoek geconcludeerd dat in de rechtspraak niet snel wordt aangenomen dat sprake is van geautomatiseerde besluitvorming (artikel 22 AVG). De onderzoekers signaleren dat het onevenwichtig kan zijn om het bewijsrisico of daarvan sprake is (geweest) geheel bij de betrokkene te leggen. Tegelijk concluderen de onderzoekers dat het prematuur is om een bepaling aan de UAVG toe te voegen, waarin de bewijslast anders wordt verdeeld, aangezien de jurisprudentie zich op dit punt nog nader moet uit kristalliseren. Ik sluit mij daarbij aan.

Tot slot hebben de onderzoekers opgemerkt dat artikel 41 UAVG, waarin uitwerking wordt gegeven aan artikel 23 AVG om de rechten van betrokkenen in te kunnen perken wegens bepaalde belangen, kan worden verbeterd zodat meer recht gedaan wordt aan de bedoeling van artikel 23 AVG. Het kabinet heeft dit ook onderkend bij de voorbereiding van het voorstel voor de Verzamelwet gegevensbescherming dat momenteel bij uw Kamer aanhangig is, en zal dit punt meenemen bij een volgende inhoudelijke wijziging van de UAVG. Dit punt is ook door de AP geadresseerd in haar brief van 23 januari 2023. Over de voortgang zal uw Kamer worden geïnformeerd. Ook in het verslag dat is uitgebracht naar aanleiding van de behandeling van de Verzamelwet gegevensbescherming zijn door verschillende Kamerleden vragen gesteld over deze bepaling en overigens ook over andere onderdelen van de brief van de AP. Die zullen in de nota naar aanleiding van het verslag uiteraard beantwoord worden.

Wetenschappelijk onderzoek

De onderzoekers stellen vast dat de regels voor het verwerken van persoonsgegevens voor wetenschappelijk onderzoek op verschillende plekken zijn neergelegd. De onderzoekers bevelen aan om de bepalingen over het verwerken van persoonsgegevens geclusterd op te nemen in de UAVG, omdat deze nu verspreid staan in de UAVG en ook te vinden zijn in sectorale wetgeving. De onderzoekers menen dat dit de uitvoerbaarheid niet bevordert.

Bij de indeling van de UAVG is de indeling van de AVG gevolgd. Hierdoor zijn de artikelen over wetenschappelijk onderzoek inderdaad in verschillende hoofdstukken terecht gekomen. Zo is er een algemeen artikel over de verwerking van bijzondere persoonsgegevens (artikel 24 UAVG), worden er nadere eisen gesteld aan de verwerking van genetische gegevens (artikel 28 UAVG), staat er een bepaling in het hoofdstuk over verwerking van strafrechtelijke gegevens (artikel 32 UAVG) en is er een

artikel in het hoofdstuk over het inperken van rechten van betrokkenen (artikel 44). Als de artikelen inzake wetenschappelijk onderzoek bij elkaar gezet worden, wordt de hoofdstukindeling van de AVG niet meer gevolgd en komen bijvoorbeeld de artikelen over de verwerking van bijzondere persoonsgegevens of de rechten van betrokkenen weer op verschillende plaatsen in de UAVG te staan. Hierdoor kunnen weer nieuwe onduidelijkheden ontstaan. Ook kunnen in sectorale wetgeving nog bepalingen omtrent wetenschappelijk onderzoek worden opgenomen, dus er kunnen altijd meerdere wetten van toepassing zijn bij de verwerking van persoonsgegevens. Het zou onwenselijk kunnen uitpakken wanneer niet meer in sectorale wetgeving specifieke concrete uitzonderingen kunnen worden opgenomen. In sectorale wetgeving kan immers een meer op de materie toegesneden norm worden opgenomen dan in de algemene UAVG. Bovendien zijn de verschillende sectoren juist bekend met hun sectorwetgeving, en naarmate er de komende jaren meer gewerkt wordt op dit onderwerp en meer bekendheid met dit instrumentarium ontstaat, zal dat de onduidelijkheid verder doen verminderen. Het is dan ook geen uitgemaakte zaak dat opneming van onderdelen uit die sectorwet in een algemene wet als de UAVG zal leiden tot meer verduidelijking.

Geautomatiseerde besluiten

De onderzoekers vragen zich af of artikel 40 UAVG recht doet aan artikel 22 AVG. In laatstgenoemd artikel is de hoofdregel neergelegd niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor de betrokkene rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft. De onderzoekers bevelen aan om een andere invulling te geven aan artikel 22 AVG dan nu in artikel 40 UAVG is opgenomen. De uitzonderingen voor geautomatiseerde besluiten zijn volgens de onderzoekers in artikel 40 UAVG namelijk erg ruim geformuleerd. Zo is geautomatiseerde besluitvorming, met uitzondering van profilering, voor overheidsorganisaties mogelijk in geval van een wettelijke verplichting of wanneer het noodzakelijk is voor de vervulling van een taak van algemeen belang. De verwerkingsverantwoordelijke moet daarbij passende waarborgen treffen. De onderzoekers menen dat van de vereiste passende waarborgen onvoldoende sprake is, nu deze vooral de mogelijkheden van bezwaar en beroep zouden behelzen en dat niet altijd toereikend is.

Ik ben mij ervan bewust dat de in artikel 40 van de UAVG gekozen implementatie van artikel 22 AVG niet de enige mogelijke uitwerking van die bepaling is. Dat betekent mijns inziens evenwel niet dat dit als een onjuiste implementatie moet worden gezien. Zoals uiteengezet in de memorie van toelichting, meen ik dat de AVG, mede gelet op overweging 71 van de AVG, deze uitwerking toelaat.¹⁰

Passende waarborgen zijn inderdaad een essentiële voorwaarde voor het gebruik van geautomatiseerde besluitvorming door overheidsorganen. De mogelijkheden van bezwaar en beroep zijn niet het enige regulerend kader voor de inzet van geautomatiseerde besluitvorming. Zo vereisen de Grondwet en het EVRM dat een inbreuk op een recht alleen is toegelaten indien deze wettelijk is geregeld en noodzakelijk en proportioneel is. Ook verbiedt het non-discriminatierecht het maken van een (ongerechtvaardigd) onderscheid. Verder stelt het bestuursrecht regels aan besluitvorming, zoals de motivering ervan en hoor en wederhoor. De overheid dient deze juridische kaders te allen tijde in acht te nemen, ook bij geautomatiseerde besluitvorming. In dit verband zijn er verschillende

¹⁰ Kamerstuk 34 851, nr. 3, blz. 46 e.v. en blz. 119 e.v.

stappen gezet om te zorgen voor aanvullende waarborgen. Allereerst werkt het kabinet aan het implementatiekader «inzet van algoritmen» dat toe moet zien op het borgen van een verantwoorde inzet van algoritmen door overheden. Het wordt daardoor voor overheden duidelijker aan welke eisen moet zijn voldaan en wat van hen verwacht wordt. Daarnaast geldt al langer het uitgangspunt dat overheidsorganisaties in beginsel geen algoritmen hanteren die te complex zijn om redelijkerwijs te kunnen worden uitgelegd, in elk geval niet indien het gebruik van algoritmen rechtsgevolgen of een aanmerkelijke impact heeft op burgers, bedrijven of (groepen in) de samenleving. Dit uitgangspunt is neergelegd in de richtlijnen voor het gebruik van algoritmen door overheden¹¹. Het kabinet wil zo transparant, consistent en controleerbaar mogelijk zijn bij de geautomatiseerde uitvoering van wet- en regelgeving. Zo wordt gewerkt aan een algoritmeregister, waarin begrijpelijke informatie wordt opgenomen over tenminste hoog risico algoritmes. De Eerste Kamer is hierover begin dit jaar bij brief separaat geïnformeerd.¹² Met betrekking tot de uitlegbaarheid van algoritmes wijs ik ook graag op het volgende. Eerder dit jaar heeft de Minister van Binnenlandse Zaken aan uw Kamer ter informatie de preconsultatieversie van het wetsvoorstel versterking waarborgfunctie Awb toegezonden.¹³ Bij deze preconsultatie zijn enkele vragen voorgelegd over algoritmische besluitvorming en hoe daarover gecommuniceerd wordt. Dit om van de aangeschreven partijen meer zicht te krijgen op de huidige praktijk. Dit onderwerp is voorts nader verkend in een expertsessie. Uiteraard wordt u hierover te zijner tijd nader geïnformeerd.

Zoals hiervoor aangegeven menen wij dat met artikel 40 UAVG niet op onaanvaardbare wijze uitvoering wordt gegeven aan artikel 22 AVG. In lijn met de vereisten op grond van deze bepalingen wordt veel in het werk gesteld om het gebruik van algoritmen bij geautomatiseerde besluitvorming met zoveel mogelijk waarborgen te omkleden en zo transparant mogelijk te laten zijn. Het denken hierover en de ervaringen in de praktijk staan evenwel niet stil. Wij zullen alles overziend steeds bezien of de bestaande waarborgen en lopende trajecten toereikend zijn om in alle fasen van besluitvorming de rechten van de burgers voldoende te verzekeren en daarop zo nodig aanvullingen voorstellen.

Minderjarigen

De onderzoekers stellen dat in het voorstel voor de Verzamelwet gegevensbescherming voor sommige toestemmingen de leeftijdsgrens wordt verlaagd naar 12 jaar. Dit is echter niet het geval. Wel wordt in het voorstel voor de Verzamelwet de leeftijdsgrens voor het *intrekken* van toestemming verlaagd naar 12 jaar, omdat die jongere niet afhankelijk zou moeten zijn van toestemming van zijn wettelijk vertegenwoordiger om een einde te maken aan de gegevensverwerking. Ook mogen kinderen van 12 jaar zelf eventueel de rechten van de betrokkene uitoefenen. De leeftijd van 12 jaar wijkt af van de leeftijdsgrens van 13 jaar, die in artikel 8 van de AVG wordt genoemd bij een rechtstreeks aanbod van diensten van de informatiemaatschappij, maar sluit goed aan bij de keuze in het Nederlands recht om kinderen vanaf 12 jaar deels zelf en vanaf 16 jaar geheel zelfstandig persoonlijke keuzes te laten maken.¹⁴ De keuze om de

¹¹ <https://www.rijksoverheid.nl/documenten/richtlijnen/2021/09/24/richtlijnen-voor-het-toepassen-van-algoritmen-door-overheden-en-publieksvoorlichting-over-data-analyse>.

¹² Brief van 16 februari 2023.

¹³ Aanbiedingsbrief bij teksten voor de preconsultatie van het wetsvoorstel versterking waarborgfunctie Awb | Rijksoverheid.nl.

¹⁴ Voor een overzicht van de in het Nederlands recht gehanteerde leeftijdsgrenzen wordt verwezen naar het advies «Leeftijdsgrenzen. Betere kansen voor kwetsbare jongeren» van de Raad voor Volksgezondheid en Samenleving van juni 2018.

leeftijdsgrens van 12 jaar op te nemen wordt daarom gehandhaafd. Overigens zijn in het verslag dat is uitgebracht naar aanleiding van de behandeling van de Verzamelwet gegevensbescherming door verschillende Kamerleden vragen gesteld over deze bepaling. In de nota naar aanleiding van het verslag zal bij de beantwoording van deze vragen dan ook nog uitgebreider op deze materie worden ingegaan.

Handhaafbaarheid

Handhaafbare normen zijn duidelijke normen, stellen de onderzoekers, en een belangrijk kenmerk van de normen uit de UAVG is dat ze niet heel duidelijk maar tamelijk open zijn geformuleerd. Naar mijn mening leent de UAVG zich niet goed voor een andere systematiek. Voor concrete normen per domein is sectorale materiewetgeving meer geëigend, zoals ook overigens de voorkeur heeft van de Raad van State in het advies bij de Verzamelwet gegevensbescherming¹⁵ en de onderzoekers ook als algemeen uitgangspunt aanbevelen.

De onderzoekers bevelen verder aan dat de toezichthouder een normenkader publiceert dat houvast geeft voor het opstellen van sectorale gedragscodes. Wij onderschrijven deze aanbeveling. Anders dan de onderzoekers zien wij echter niet dat een verplichting daartoe in de UAVG de manier zou zijn om dit te realiseren. Zo'n verplichting zou op gespannen voet staan met het onafhankelijke karakter van de toezichthouder. Hoewel een duidelijk normenkader zonder meer nuttig is, is het aan de onafhankelijke toezichthouder om te bepalen op welke wijze daaraan vorm en inhoud gegeven wordt.

Onderdeel 2: De meldplicht datalekken en de boetebevoegdheid in de praktijk

Met de evaluatie van deze instrumenten (die beide per 1 januari 2016 in de Wbp zijn gevoegd en in werking getreden) wordt invulling gegeven aan de motie Schouw en Segers uit 2015. De onderzoekers hebben het functioneren van beide instrumenten beoordeeld aan de hand van interviews en praktijkonderzoek.

Algemeen

Over het toezichtsproces in zijn algemeenheid merken de onderzoekers op dat het lastig is om uit de onderzochte casus duidelijke regelmatigheden te onderkennen. Er is naar het oordeel van de onderzoekers geen eenduidigheid in het optreden van de toezichthouder, in de zin dat dit bijvoorbeeld begint met informeel contact en via een aantal stappen escaleert naar een handhavingsbesluit. De escalatieladder ziet er in de onderzochte gevallen telkens anders uit. De onderzoekers valt op dat op het terrein van het gegevensbeschermingsrecht sprake is van veel onduidelijkheid over de normen alsook veel onbegrip over het optreden van de toezichthouder. De vaste bestuurspraktijk is er een waarbij de AP doorgaans geen overleg voert, omdat het principe wordt gehanteerd dat de toezichthouder niet onderhandelt. Tegelijk hebben ondertoezichtgestelden veelal behoefte aan normuitleg en duiding. Contacten met de toezichthouder zouden, ook in handhavingszaken, tot veel verheldering kunnen leiden en kunnen voorkomen dat toezichthouder en onder toezicht gestelde in een verscherpte verhouding tegenover elkaar komen te staan, aldus de onderzoekers. Het lijkt de onderzoekers daarom verstandig dat hiertoe beleid wordt ontwikkeld, zogenoemd toezichtbeleid, dat in beleidsregels wordt opgenomen en dat op die manier kenbaar is voor

¹⁵ Kamerstuk 36 264, nr. 4.

ondertoezichtgestelden. Het zou volgens hen denkbaar zijn dat in de UAVG wordt voorgeschreven dat de toezichthouder beleidsregels bekendmaakt, waarbij in een voorafgaande consultatieprocedure van belanghebbenden voorzien zou kunnen worden.

Terecht stellen de onderzoekers vast dat het van groot belang is voor het draagvlak en de effectiviteit van het toezichtsproces dat daarover duidelijkheid en kenbaarheid bestaat. Het is evenwel niet de wetgever maar in de eerste plaats aan de toezichthouder om te reflecteren op deze aanbeveling. Het opnemen van een verplichting in de UAVG voor de AP om beleidsregels bekend te maken, raakt aan de onafhankelijkheid van de AP en is daarmee geen optie die nader zal worden verkend. Wel zal ik het belang van een kenbaar toezichtskader onder de aandacht brengen van de AP.

De meldplicht datalekken

Over de werking van de meldplicht datalekken verwijzen de onderzoekers naar de door de AP zelf in haar jaarverslag van 2021 reeds geuite zorg dat er nauwelijks capaciteit is om ernstige datalekken te onderzoeken en dat ook meer in het algemeen veel meldingen van datalekken niet opgepakt kunnen worden. Verder stellen de onderzoekers vast dat de AP in een minderheid van de gevallen reageert op een melding. Ook is het de onderzoekers opgevallen dat het tijdig melden van een datalek geen rol speelt bij het bepalen van de boetehoogte, wat verwerkingsverantwoordelijken geen positieve prikkel zou geven om eigener beweging een melding te doen, temeer nu de pakkans laag is in geval van niet melden.

Uit het onderzoek komt tevens naar voren dat de AP zelf zoekt naar mogelijkheden om haar toezicht op de meldplicht datalekken te verbeteren en haar capaciteit zo goed mogelijk daarop in te zetten. In het Coalitieakkoord is extra budget voor de AP opgenomen dat oploopt tot 8 miljoen euro structureel per jaar in 2025. De AP kan dit budget naar eigen inzicht besteden over zijn taken. Het is niet aan het kabinet om hierin te treden, omdat de AP onafhankelijk is in de wijze waarop zij haar taken en bevoegdheden uitoefent.

De boetebevoegdheid

Ten aanzien van de boetebevoegdheid van de AP stellen de onderzoekers vast dat beleidsregels waarin het toezichts- en handhavingsbeleid is vastgelegd ontbreken en dat daardoor geen sprake is van kenbaar beleid op dit punt. Met name is onduidelijk op welke wijze de toezichthouder een escalatiestrategie toepast. Dit punt kwam ook al terug in de bevindingen met betrekking tot het toezichtsproces in zijn algemeenheid. Voorts is niet inzichtelijk hoe het beleid over de matiging van boetes in de praktijk wordt toegepast.

De rechtszekerheid heeft zonder meer baat bij een zekere mate van voorspelbaarheid inzake het opleggen van een administratieve boete. Het moet voor iedereen duidelijk zijn op welke consistente gronden dit gebeurt en hoe in verschillende situaties met de wegingscriteria wordt omgegaan. Zoals gezegd is het aan de AP zelf om te bepalen welke opvolging aan de aanbevelingen van de onderzoekers zal worden gegeven. De toezichthouder heeft hier een autonome afwegingsruimte waarin ik niet kan treden.

Voorts memoreren de onderzoekers dat er geen beleid is gepubliceerd door de AP met betrekking tot het publiceren van handhavingsbesluiten. Publicatie zou volgens de onderzoekers de normnaleving kunnen

bevorderen en de preventieve werking dienen. De wetgever heeft de toezichthouder tot op heden ook niet verplicht boetebesluiten te publiceren, aldus de onderzoekers.

Ook voor het opleggen van deze verplichting laat de eerdergenoemde zelfstandigheid van de AP geen ruimte. Wel is het belang evident van het punt dat de onderzoekers naar voren brengen. Ik zal ook hierover met de AP in gesprek gaan.

Tot slot pleiten de onderzoekers ervoor om in de UAVG de verplichting op te nemen dat boetebesluiten jegens bestuursorganen, door de AP openbaar worden gemaakt. Dat zou kunnen bijdragen aan het aanhouden van een consistente lijn rondom openbaarmaking van sancties en dienend zijn aan het belang dat met openmaking daarvan gemoeid is. Bovendien geven openbaar gemaakte sancties inzicht in hoe bepaalde open normen in de praktijk door de toezichthouder worden toegepast en kan (de dreiging van) openbaarmaking bijdragen aan de beoogde generale preventieve werking van boetes.

In de eerdergenoemde brief van 23 januari 2023 heeft de AP eveneens gepleit voor een plicht tot openbaarmaking van sancties in de UAVG. Zij verwijst naar de bijzondere openbaarmakingsplichten die andere toezichthouders zoals de ACM, AFM en DNB hebben voor sancties. De AP verwijst naar de mededeling van de toenmalige Minister voor Rechtsbescherming dat het – gelet op het beleidsneutrale karakter ervan – tijdens de totstandkoming van de UAVG niet voor de hand lag om dit in de UAVG op te nemen en het bovendien in de rede lag om dit onderwerp nader te bezien als er duidelijkheid was over de voortgang van het initiatiefwetsvoorstel Wet open overheid (hierna: Woo). De Woo is per 1 mei 2022 in werking getreden, zodat het volgens de AP voor de hand ligt om te kijken naar de wenselijkheid van wijziging van de UAVG op dit punt en om ook voor de AP in de wet een verplichting tot openbaarmaking van sancties op te nemen. Ik zal de aanbeveling van de onderzoekers en het voorstel van de AP in onderlinge samenhang nader onderzoeken.

Tot slot stellen de onderzoekers dat de Functionarissen Gegevensbescherming (FG) nog te weinig een speler zijn in een handhavingscasus. Wanneer de FG de vooruitgeschoven post zou zijn van de AP past daarbij ook een speciale relatie met de externe toezichthouder, stelt het onderzoek. De AP heeft op 24 juni 2021¹⁶ uitgangspunten gepubliceerd voor het inrichten van sterk intern toezicht. In dit document wordt op onderdelen ook stilgestaan bij de relatie tussen de AP en FG's. Daarmee wordt in belangrijke mate tegemoetgekomen aan de wens van de onderzoekers.

Conclusie

Het onderzoek geeft een goed beeld van de manier waarop de UAVG in de praktijk wordt toegepast, alsook in welke mate de meldplicht datalekken wordt nageleefd en in hoeverre de boetebevoegdheid van de toezichthouder bijdraagt aan een doelmatige en doeltreffende uitvoering en handhaving van de AVG. De onderzoekers concluderen dat de UAVG in beperkte mate toegevoegde inhoudelijke waarde heeft ten opzichte van de AVG, vanwege de beperkte tijd die voor de totstandkoming beschikbaar was en de keuze voor een «beleidsneutrale» omzetting van de bestaande normen die destijds is gemaakt. Tegelijk volgt uit de interviews die de

¹⁶ <https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-publiceert-uitgangspunten-voor-inrichten-sterk-intern-toezicht>.

onderzoekers hebben afgenomen dat professionals over het algemeen goed uit de voeten kunnen met de UAVG.

De onderzoekers doen enkele voorstellen om de UAVG uit te breiden. Enkele daarvan zijn reeds meegenomen bij het wetsvoorstel Verzamelwet Gegevensbescherming, zoals biometrische gegevensverwerking en de positie van minderjarigen. Andere voorstellen zullen nader worden onderzocht op wenselijkheid en haalbaarheid en in samenhang worden bekeken met de voorstellen die de AP in haar brief van 23 januari 2023 heeft gedaan en mogelijk andere wenselijke aanpassingen van de UAVG in de toekomst.

De Minister voor Rechtsbescherming,
F.M. Weerwind