



Reactie van de Vereniging voor Informaticarecht Advocaten (**VIRA**)

“Uitvoeringswet dataverordening”

1 april 2024

De Vereniging Informaticarecht Advocaten (VIRA) heeft kennis genomen van het voorstel voor een Uitvoeringswet dataverordening. De VIRA onderschrijft het belang bij het juist implementeren en uitvoeren van de dataverordening, maar heeft twijfels op een aantal punten in het voorstel voor de Uitvoeringswet zoals deze er op dit moment ligt.

Vraagtekens en zorgen hebben wij met name op de punten waar de Algemene Verordening Gegevensbescherming (AVG) en de Dataverordening elkaar raken of in elkaars vaarwater komen. Die zorgen worden vergroot door de respectievelijke bevoegdheid van de twee toezichthouders: de Autoriteit Persoonsgegevens (AP) en de Autoriteit Consument en Markt (ACM). Hoewel samenwerking tussen beide toezichthouders is voorgeschreven en voor de hand ligt, en zelfs bepaald wordt dat onderling gegevens mogen worden uitgewisseld, weten en ervaren we in de huidige praktijk van alledag dat die samenwerking in het toezicht niet vanzelfsprekend of logisch is, met alle gevolgen van dien voor de rechtszekerheid. De VIRA plaatst dan ook haar vraagtekens bij de gevolgen van deze Uitvoeringswet voor de slagkracht en daadkracht van de toezichthouder(s) en daarmee voor de algehele rechtszekerheid. Onze vragen op deze punten worden niet beantwoord in het wetsvoorstel, noch in het ontwerp voor de Memorie van Toelichting.

In het hierna volgende lichten we de volgende zorgen toe:

1. Zorgen rechtszekerheid over delen van data/gegevensuitwisseling (*free flow of data*)
2. Wie bepaalt de norm?
3. Rechtsongelijkheid: zorgen over verschillende normuitleg door ACM resp. AP
4. ‘Toestemming’ is onjuist
5. Wie legt wanneer welke boete op? ACM 10% of AP 4% van wereldwijde omzet?
6. Rechtszekerheid in het geding
7. Burger beschermd? Klacht en oplossing door wie?
8. De geschillencommissie
9. Certificering door wie?
10. Samenwerkingsprotocol – klagen bij wie?
11. Rechtbank Rotterdam exclusief bevoegd
12. Evaluatie
13. Conclusie

1. Zorgen rechtszekerheid over delen van data/gegevensuitwisseling (*free flow of data*)

Zoals al kort aangegeven, onze zorgen komen voornamelijk voort uit het spanningsveld tussen de Dataverordening en de AVG. De Dataverordening bepaalt op diverse plaatsen expliciet dat géén afbreuk wordt gedaan aan de AVG, maar dat de Dataverordening de AVG juist aanvult.¹ Voor meerdere bepalingen en voorzieningen betekent dit dat er een algemene regel wordt gegeven in de AVG, en dat er een specifiekere regel wordt gegeven in de Dataverordening.

Dit spanningsveld kan tot grensconflicten leiden, zoals ook in de literatuur wordt onderschreven.² Denk daarvoor bijvoorbeeld aan een situatie waarin een verzoek om gegevens tegelijkertijd kwalificeert als een uitoefening van het recht op gegevensoverdraagbaarheid onder de AVG (*dataportabiliteit*) en als een uitoefening van

¹ Zie daarvoor bijvoorbeeld overwegingen 7, 20, 31, 34, 35, 39, 45, 69 en 94 en artikel 1 lid 5 van de Dataverordening.

² Zie daarvoor bijvoorbeeld L. Deschuyteneer & A. Van de Meulebroucke, ‘Interacties tussen de Data Governance Act, de Data Act en de Algemene Verordening Gegevensbescherming: een nieuwe koers of een geëffend pad?’, *Computerrecht* 2023/115.

het recht op toegang tot gegevens onder de Dataverordening. Die grensconflicten tussen AVG en zullen naar onze verwachting in praktijk aan de orde van de dag zijn.

2. Wie bepaalt de norm?

Zorgen over samenwerking en (conflicterende) bevoegdheid tussen de twee toezichthouder(s) AP en ACM

In het wetsvoorstel wordt de ACM aangewezen als datacoördinator en bevoegde autoriteit op alle onderdelen van de verordening behalve hoofdstuk 5, dat betrekking heeft op het beschikbaar stellen van gegevens aan overheidsinstanties en EU-instellingen in gevallen van uitzonderlijke noodzaak. De AP wordt aangewezen als de bevoegde autoriteit op dit hoofdstuk 5, en de rol van toezicht van de AP is daarmee onder deze wet beperkt tot – kort gezegd – de overheid.

Toch ligt hier een uitdaging; zoals terecht in de Memorie van Toelichting (MvT) wordt opgemerkt, heeft de Dataverordening zowel betrekking op persoonsgegevens als niet-persoonsgebonden gegevens. In paragraaf 5.1 van de MvT wordt over deze samenloop het volgende opgemerkt:

“5.1 Algemene verordening gegevensbescherming

Deze verordening doet geen afbreuk aan Unierecht en het nationale recht inzake de bescherming van persoonsgegevens, de persoonlijke levenssfeer en de vertrouwelijkheid van communicatie en de integriteit van eindapparatuur, die van toepassing zijn op persoonsgegevens die worden verwerkt in verband met de hierin vastgelegde rechten en verplichtingen met inbegrip van de bevoegdheden van toezichthoudende autoriteiten en de rechten van datasubjecten. De verordening doet in het bijzonder geen afbreuk aan de Algemene Verordening Gegevensverwerking (AVG).

Bij verwerking van persoonsgegevens is de regelgeving met betrekking tot persoonsgegevens altijd van toepassing en bij tegenstrijdigheid met de verordening prevaleert de regelgeving met betrekking tot persoonsgegevens. Dit geldt ook voor de situatie waarin persoonsgegevens en andere gegevens in een gegevensverzameling onlosmakelijk met elkaar verbonden zijn. De Autoriteit Persoonsgegevens (AP) is de toezichthouder met betrekking tot persoonsgegevens op basis van de AVG, en blijft dat. Wanneer bijvoorbeeld is beoordeeld dat het delen van gegevens conform hoofdstuk II van de verordening heeft plaatsgevonden, verhindert dat geenszins de AP om de rechtmatigheid van deze dataverwerking conform de AVG te beoordelen.”

En deze samenloop gaat nog iets verder zoals terecht in de MvT opgemerkt:

“Beginselen rechtmatige gegevensverwerking

De verordening regelt dat een aantal beginselen voor rechtmatige gegevensverwerking uit artikel 5 van de AVG ook (deels) van toepassing worden op niet-persoonsgebonden gegevens die zijn gegeneerd met een verbonden product of gerelateerde dienst en op verzoek van de gebruikers worden gedeeld met een derde partij (artikel 6 van de verordening).”

Met andere woorden, de norm-uitleg van begrippen uit de AVG die gelden voor persoonsgegevens spelen ook een rol bij de uitleg van begrippen voor niet-persoonsgegevens.

Hierin ligt een uitdaging: Kan de ACM bijvoorbeeld wel een normuitleg voor het recht op toegang tot gegevens uitvaardigen, als de AP al een normuitleg voor het recht op gegevensoverdraagbaarheid hanteert?

De Uitvoeringswet komt aan dit probleem slechts deels tegemoet door te bepalen dat de ACM advies kan vragen aan de AP (artikel 5), zowel in het kader van de verplichting tot loyale samenwerking en ook bij een norm-uitleg. Maar de vraag is of dit voldoende is.

Met name nu is bepaald (en volgens de MvT kennelijk bedoeld (par. 4.3)) dat de ACM niet hoeft te wachten op de AP totdat deze tijd heeft. De ACM kan aldus zelf en mogelijk tegenstrijdig een norm uitleggen; hetgeen andersom des te meer geldt. Immers, een vergelijkbare regel geldt niet in de omgekeerde richting; de AP moet of hoeft de ACM niet om advies te vragen indien zij een normuitleg opstelt die ook effect heeft op verwerking of uitwisseling van niet-persoonsgegevens. En dat is reden voor grote zorg, zie daarvoor de voorbeelden en onze opmerkingen hierna waarbij de AP op geheel eigenzinnige wijze uitleg geeft aan Europese normen.

3. Rechtsongelijkheid: zorgen over verschillende normuitleg door ACM resp. AP

De Dataverordening stuurt op een *free flow of data* en een stimulering van het verdere gebruik van gegevens. Waar gegevens “persoonsgegevens” zijn, is daarvoor een rechtmatige grondslag nodig zoals bedoeld in de AVG.

Een rechtmatige grondslag om persoonsgegevens te verwerken voor behartiging van de belangen van een ‘verwerkingsverantwoordelijke’ of een ‘derde’ is bijvoorbeeld de grondslag “gerechtvaardigd belang” (artikel 6 lid 1 sub f AVG):

“f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.”

Hoewel de AVG daarmee de rechtmatige grondslag biedt voor een “free flow of data” en ook de belangen van derden daarbij benoemt, legt de AP de bedoelde gegevensuitwisseling sterk aan banden en beperkt zij deze nagenoeg volledig door haar huidige normuitleg op dit punt. Volgens die AP uitleg is gegevensuitwisseling voor ‘zuiver commerciële’ belangen van een verwerkingsverantwoordelijke of van een derde niet mogelijk.

De Uitvoeringswet lost dit probleem niet op, maar laat de ruimte voor de situatie waarin het mogelijk is dat de twee verschillende toezichthouders zeer uiteenlopende visies ontwikkelen op gelijke of vergelijkbare normen op hetzelfde toepassingsgebied.

Ons advies is daarom om op dit punt van samenwerking tussen beide aangewezen autoriteiten nader duiding te geven in de Uitvoeringswet.

4. ‘Toestemming’ is onjuist

In de MvT is onterecht en onjuist opgenomen dat een datasubject (‘betrokkene’ onder de AVG) toestemming zou moeten geven voor gegevensuitwisseling en verdere verwerking zoals bedoeld is in de Dataverordening.

Deze alinea met betrekking tot rechtmatigheid van verdere verwerking van gegevens in paragraaf 5.1 van de MvT is onjuist:

Rechtmatig: de derde mag die gegevens alleen met een andere derde delen indien de gebruiker daar toestemming voor heeft gegeven.

~~Bovendien moet het voor de gebruiker even gemakkelijk zijn om toegang van de derde tot de gegevens te weigeren of stop te zetten als het voor de gebruiker is om toegang te verlenen.~~

In artikel 6 van de Dataverordening is het volgende bepaald:

Artikel 6 Verplichtingen van derden die op verzoek van de gebruiker gegevens ontvangen

1. Een derde verwerkt de hem overeenkomstig artikel 5 ter beschikking gestelde gegevens uitsluitend voor de doeleinden en onder de voorwaarden die met de gebruiker zijn overeengekomen, en met inachtneming van het Unierecht en het nationale recht inzake de bescherming van persoonsgegevens, met inbegrip van de rechten van het datasubject wat persoonsgegevens betreft. De derde wist de gegevens wanneer zij niet langer noodzakelijk zijn voor het overeengekomen doel, tenzij in verband met niet-persoonsgebonden gegevens anders met de gebruiker is overeengekomen.

In de Dataverordening is aldus opgenomen dat een derde alleen gegevens verwerkt “onder de voorwaarden die met de gebruiker” zijn overeengekomen. Dat veronderstelt een ‘overeenkomst’ (en daarmee de grondslag “uitvoering van een overeenkomst” zoals

bedoeld in artikel 6 lid 1 sub b AVG). In de Dataverordening is daarmee zeker niet enkel “toestemming” bedoeld (zoals bedoeld in artikel 6 lid 1 sub a AVG), maar wordt verwezen naar de AVG in het algemeen en daarmee geldt dat één van de in de AVG limitatief opgesomde rechtmatige grondslagen van toepassing moet zijn. Het onderscheid is van wezenlijk belang; enkel verwijzen naar de grondslag “toestemming” is onnodig beperkend voor een verdere gegevensuitwisseling zoals in de Dataverordening is bedoeld.

Ten aanzien van het verstrekken van toegang tot gebruiksgegevens: in de Dataverordening is niet bepaald dat het stoppen of weigeren van toegang voor een derde door een gebruiker even gemakkelijk moet zijn als de mogelijkheid tot het verlenen van toegang door die gebruiker. In de Dataverordening is het volgende bepaald (artikel 6 lid 2):

2. De derde: a) maakt de uitoefening van het maken van keuzes of rechten uit hoofde van artikel 5 en dit artikel door gebruikers niet onnodig moeilijk door onder meer keuzemogelijkheden op niet-neutrale wijze aan de gebruiker te presenteren, hen te dwingen, te misleiden of te manipuleren, of door de autonomie, besluitvorming of keuzes van de gebruiker te ondermijnen, onder meer met behulp van een digitale gebruikersinterface met de gebruikers of een deel daarvan;

Deze bepaling in de Dataverordening is veel meer een verbod op ‘nudging’ en sluit meer aan bij het verbod op misleidende reclame, dan op een ‘gebod’ om toegang in te trekken even gemakkelijk te laten zijn als het verlenen van toegang.

De in de MvT opgenomen zin ten aanzien van toegangsverlening aan een derde door een gebruiker lijkt bedoeld om aansluiting te zoeken bij de bepaling in de AVG dat het intrekken van toestemming even gemakkelijk dient te zijn als het verlenen van toestemming (artikel 7 lid 3 AVG). Echter “toestemming” is niet de meest voor de hand liggende rechtmatige grondslag voor gegevensuitwisseling onder de Dataverordening. De Dataverordening lijkt dat ook niet te bedoelen omtrent de verlening van toegang tot gebruiksgegevens door een derde, daarmee is de vraag waar deze uitleg in de MvT vandaan komt.

In artikel 5 lid 7 van de Dataverordening is expliciet bepaald dat gegevens van personen kunnen worden verwerkt indien deze niet rechtstreeks van hen zijn verkregen (gelijk de AVG daarvoor voorzieningen kent), mits daarvoor een rechtmatige grondslag zoals bedoeld in artikel 6 lid 1 van de AVG is. De grondslag “toestemming” zal ook dan niet vaak van toepassing kunnen zijn, cq deze kan geen toepassing vinden omdat de derde met de

betrokkene geen rechtstreekse relatie onderhoudt en dus niet zelf om toestemming kan vragen:

7. Wanneer de gebruiker niet het datasubject is van wie de persoonsgegevens worden opgevraagd, worden persoonsgegevens die door het gebruik van een verbonden product of een gerelateerde dienst zijn gegenereerd alleen door de gegevenshouder ter beschikking gesteld van de derde indien er een geldige rechtsgrond voor verwerking bestaat uit hoofde van artikel 6 van Verordening (EU) 2016/679 en, in voorkomend geval, indien aan de voorwaarden van artikel 9 van die verordening en van artikel 5, lid 3, van Richtlijn 2002/58/EG is voldaan.

In praktijk zal voor dergelijke gevallen meestal de grondslag “gerechtvaardigd belang” van toepassing zijn. Daarbij is vereist dat er een gerechtvaardigd belang toets wordt doorlopen, zoals is bedoeld onder de AVG. Het verdient aanbeveling in de MvT een opmerking ten aanzien van deze verwerkingen op basis van deze grondslag “gerechtvaardigd belang” op te nemen in de verhouding tot gegevensuitwisseling onder de Dataverordening.

5. Wie legt wanneer welke boete op? ACM 10% of AP 4% van wereldwijde omzet?

De wetgever maakt de keuze om in de Uitvoeringswet een boetemaximum van 10% van de wereldwijde jaaromzet in te stellen. Hierbij staat het boetemaximum van 4% die onder de AVG mag worden opgelegd in schril contrast.

Als een organisatie door dezelfde gedraging de AVG én de Dataverordening schendt, kan hem dus door de ACM een boete worden opgelegd van 10%, en door de AP een boete worden opgelegd van 4%. Wanneer hierbij ook in het achterhoofd wordt gehouden dat de ACM en de AP niet dezelfde boetebeleidsregels hanteren, ontstaat het beeld dat een organisatie simpelweg niet weet wat zij kan verwachten bij de handhaving van de Dataverordening en de AVG.

In de Dataverordening wordt ten aanzien van mogelijke boetes aansluiting gezocht bij het bepaalde in de AVG (artikel 40 lid 4 Dataverordening). Waarom de Uitvoeringswet een ander (hoger) maximum hanteert van 10% van de wereldwijde jaaromzet, zoals de ACM deze al kent bij handhaving van de Telecommunicatiewet, is in de MvT zeer mager gemotiveerd (in par. 4.2). De MvT geeft geen duidelijke verklaring waarom door de wetgever in de Uitvoeringswet van het bepaalde in de Dataverordening wordt afgeweken.

Bovendien creëert de wetgever met de bepaling in de Uitvoeringswet dat zowel de AP als de ACM boetes mogen opleggen tot 10% van de wereldwijde jaaromzet. Dat betekent dat

door het bepaalde in de Uitvoeringswet ook de AP een bevoegdheid verkrijgt om hoger te sanctioneren dan waartoe zij bevoegd is onder de AVG. Wij vragen ons af of die verruimde boetebevoegdheid voor de AP ook op die wijze is bedoeld met het bepaalde in de Uitvoeringswet.

6. Rechtszekerheid in het geding

Niet alleen leidt de keuze voor het aanwijzen van twee toezichthouders tot afstemmingsproblemen die aan de zijde van de overheid tot een gebrek aan daadkracht kunnen leiden, maar aan de zijde van de burger leidt dit tot een risico van grote rechtsonzekerheid.

Dit vloeit voort uit het feit dat de twee kapiteins op één schip dezelfde regels verschillend kunnen handhaven. Denk hierbij bijvoorbeeld aan de situatie waarin een persoon bepaalde gegevens opvraagt uit hoofde van de Dataverordening, en de gegevenshouder dit weigert, omdat hij stelt dat hij de gegevens reeds heeft vernietigd indachtig het beginsel van gegevensminimalisatie uit de AVG. Als het datasubject hierover een klacht indient bij de ACM, zal de ACM onder andere de norm van gegevensminimalisatie, en dus de AVG, moeten uitleggen en interpreteren.³ Dit wordt schrijnend wanneer ook daadwerkelijk boetes worden opgelegd: kan een organisatie vertrouwen op de normuitleg van de ene toezichthouder, wanneer hij wordt bestraft door de andere? Het onderliggende “issue” lijkt de onafhankelijkheid van de AP te zijn en dat wordt vergroot door verschillende toezichthouders aan te wijzen. Het lijkt ons echter niet dat het belang van de onafhankelijkheid van de AP zwaarder zou mogen wegen dan het belang van de materiële en formele rechtszekerheid.

7. Burger beschermd? Klacht en oplossing door wie?

Overeenkomstenrecht

In de MvT wordt terecht opgemerkt dat op basis van het beginsel van contractvrijheid het partijen blijft vrijstaan om te onderhandelen over de precieze voorwaarden voor het beschikbaar stellen van gegevens in hun overeenkomsten, binnen het kader van algemene regels voor het beschikbaar stellen van gegevens (par. 5.5). Dat geldt ook voor de overeenkomst met consumenten:

³ De Dataverordening erkent dit spanningsveld ook in overweging 24.

De overeenkomst voor de aankoop, huur of leasing van een verbonden product of gerelateerde dienst vormt de basis voor het gebruik van niet-persoonsgebonden gegevens. Elke contractvoorwaarde die bepaalt dat de gegevenshouder de productgegevens of de gegevens van een gerelateerde dienst mag gebruiken, moet transparant zijn voor de gebruiker, ook over de doeleinden waarvoor de gegevenshouder de gegevens zal gebruiken. ~~Elke wijziging van de overeenkomst vereist de geïnformeerde toestemming van de gebruiker.~~

Onjuist is echter dat iedere wijziging van een overeenkomst – ook als die overeenkomst met een consument (en daarmee data subject of ‘betrokkene’) is gesloten – “*de geïnformeerde toestemming van de gebruiker*” is benodigd. Dat is niet het geval.

Ook zonder “geïnformeerde toestemming” kan een overeenkomst worden gewijzigd. Nodig is dat de andere partij in zijn voorwaarden (en daarmee overeenkomst) een wijzigingsbeding heeft opgenomen, waarbij vervolgens nog geldt dat 1) een wijziging redelijk is, 2) de nieuwe voorwaarden kenbaar zijn gemaakt aan de consument (toegestuurd) en 3) na de vaste looptijd ingaan. Indien de andere partij zich niet aan deze eisen houdt, kan een consument de aanpassing in de overeenkomst ongeldig maken (laten vernietigen)^{4, 5}.

Relatie consumentenrecht

In de MvT wordt in par. 5.5 terecht opgemerkt dat privaatrechtelijke regels van cruciaal belang zijn in het algemene kader voor gegevensdeling. Dat is niet alleen om “*een eerlijke toegang tot en een eerlijk gebruik van gegevens*” te borgen, maar ook om consumenten te beschermen.

Het toezicht van ACM bouwt voort op het private fundament van brancheorganisaties en Stichting Reclame Code. Sinds de jaren ’70 bestaan er ca. 50 geschillencommissies, georganiseerd per economische sector, die de belangrijkste economische sectoren bestrijken, zoals het bankwezen, energie, telecommunicatie, online winkelen en reizen. Deze geschillencommissies zijn een vorm van zelfregulering, aangevuld met door de overheid goedgekeurde procedures. Consumenten hebben directe toegang tot de commissies en het advies is in beginsel bindend voor beide partijen.

Bovenop dit private fundament in het consumentenrecht geldt dat de consument een beroep kan doen op de burgerlijke rechter om zijn rechten te laten gelden⁶.

⁴ <https://www.acm.nl/nl/verkoop-aan-consumenten/de-koop-sluiten/algemene-voorwaarden-aanbieden>

⁵ Artikel 6:233 en verder Burgerlijk Wetboek

⁶ <https://www.acm.nl/nl/publicaties/publicatie/12288/Speech-Anita-Vegter-over-consumententoezicht-in-Nederland>

Dit privaatrechtelijke fundament geldt nog steeds en daarmee heeft de consumentenbescherming in Nederland een traditie van dialoog en samenwerking, aldus ook de ACM:

“De wet handhaving consumentenbescherming van 2008 bouwde voort op bestaande zelfregulering die in co-creatie tussen consumentenorganisaties en bedrijven tot stand was gekomen. Denk aan de stichting reclamecode en de geschillencommissies. Het private fundament was de basis, publiekrechtelijk toezicht en publiekrechtelijke handhaving de kop daarbovenop. De wet voorzag dat de Consumentenautoriteit en later haar opvolger ACM pas in actie zou komen wanneer inbreuken op het consumentenrecht collectief waren, én wanneer het private fundament niet effectief was. De wet voorzag ook in nauwe samenwerking tussen de publiekrechtelijke handhaver en de bestaande private initiatieven.”

Tussen de ACM en Stichting Reclame Code bestaat ook een samenwerkingsprotocol⁷.

De vraag is nu op welke wijze dit private fundament van consumentenbescherming, consumentenrecht en deze geschillencommissies zich nu verhouden tot het bepaalde in de Dataverordening. Op welke wijze is de burger nu beschermd? Cq waar dient deze zijn klacht in te dienen?

8. De geschillencommissie

De ACM is bevoegd een geschillenbeslechtsorgaan te certificeren; dit leidt tot een privaatrechtelijke oplossing. Hoe verhoudt deze zich tot het toezicht door de ACM dan wel AP? Betekent een ‘opgeloste klacht’ geen boete?

Er is in de Uitvoeringswet bepaald dat de ACM geschilbeslechtsers kan certificeren (artikel 2 Uitvoeringswet) zoals bedoeld in artikel 10 lid 5 van de Dataverordening. De MvT vermeldt dat geen gebruik wordt gemaakt van de ruimte die de Dataverordening voor dergelijke nationale regels biedt (par. 4.4, pagina 17 laatste zin), maar erg overtuigend is dit niet.

Hoewel kennelijk bedoeld is om nadere kaderstelling voor certificering van een geschillenbeslechtsorgaan achterwege te laten, is een overweging of de bestaande – op basis van zelfregulering met privaat fundament ingestelde - commissies een rol kunnen of zouden moeten spelen in geschillenbeslechting over geschillen onder de Dataverordening naar onze mening op zijn plaats.

Daarbij verdient ook het toezichthoudend orgaan op AVG gedragscodes zoals bedoeld in artikel 41 AVG een opmerking van de wetgever. Ook dit instituut wordt benoemd met een

⁷ <https://zoek.officielebekendmakingen.nl/stcrt-2016-32094.html>

rol in geschillenbeslechting bij klachten; dit toezichthoudend orgaan wordt door de AP geaccrediteerd tegen (zware) vastgestelde accreditatiecriteria. Is een door de AP 'geaccrediteerd toezichthoudend orgaan' onder de AVG eveneens direct een 'gecertificeerd geschillenbeslechtingsorgaan' onder de Dataverordening? Een nadere overweging van de wetgever lijkt op dit punt op zijn plaats.

Dat de wetgever in de MvT overweegt dat de criteria ten aanzien van certificering uit artikel 10 lid 5 Dataverordening geen nationale implementatie dan wel interpretatie vergen is verder nog maar de vraag. Al was het maar omdat per lidstaat zal verschillen wat nu eigenlijk wordt verstaan onder deskundigheid, wat een redelijke vergoeding voor de werkzaamheden is en hoe gemakkelijke elektronische toegankelijkheid wordt geborgd. Mogelijk dat de wetgever heeft bedoeld dat de ACM hiervoor beleidsregels kan opstellen,⁸ maar het is de vraag of het gelet op de trias politica wenselijk is dat normstelling, uitvoering en handhaving in één hand komen te liggen.

9. Certificering door wie?

In lijn daarmee is ook de vraag of het wenselijk is dat de certificering van geschilbeslechters en de handhaving in één hand liggen. Er kan dan immers al snel het beeld ontstaan dat de geschilbeslechter is "goedgekeurd" door de handhavende instantie. Dit terwijl de visie van de geschilbeslechter en de visie van de ACM op de interpretatie van de wet kan verschillen. Wat moet er bij een dergelijk verschil van inzicht gebeuren? Moet de ACM dan de certificering intrekken? Daar lijkt geen grond voor te zijn.

Is het niet zuiverder om de certificering van geschilbeslechters te laten doen door een instantie die zelf aan alternatieve geschilbeslechting doet? Dan zal het beeld ontstaan dat de geschilbeslechter louter op procesmatige gronden is goedgekeurd (en niet op inhoudelijke gronden).

De geschilbeslechter krijgt van de EU-wetgever bovendien uitdrukkelijk de ruimte om eigen aanbevelingen te publiceren over "*de wijze waarop problemen kunnen worden voorkomen of opgelost*" (artikel 10 lid 11 Dataverordening). Het ligt voor de hand dat dergelijke publicaties ook wetsinterpretaties zullen (gaan) bevatten. Er kan dan de wonderlijke situatie gaan ontstaan dat er wetsvisies gaan circuleren van die (door ACM goedgekeurde) geschilbeslechters, de ACM en de AP.

⁸ Vgl. artikel 4:81 e.v. Awb.

10. Samenwerkingsprotocol – klagen bij wie?

Hoewel in de MvT wordt onderkend dat het begrip “klacht” in de Dataverordening een autonome betekenis heeft, die moet worden onderscheiden van het begrip “klacht” in de Algemene wet bestuursrecht (hierna: Awb) (in par. 4.2), zijn verdere opmerkingen op dit punt nagelaten.

In artikel 5 lid 3 van de Uitvoeringswet is opgenomen dat de AP en ACM samenwerkingen kunnen aangaan met andere toezichthouders, waaronder “sectorale toezichthouders”.

Zijn andere “sectorale toezichthouders” ook de “toezichthoudende organen” zoals bedoeld in artikel 41 AVG, die door de AP zijn geaccrediteerd? Of zijn dit mogelijk ook de “gecertificeerde geschillenbeslechtsorganen”?

En zo ja, wat zijn dan de overwegingen op dit punt, wetende dat de ACM al een bestaand samenwerkingsprotocol kent en de AP dergelijke samenwerkingsprotocollen weigert aan te gaan met een beroep op haar onafhankelijkheid.

Daarbij eveneens in overweging nemend dat de ACM klachten als een signaal beschouwt en niet iedere klacht individueel zal afdoen, terwijl de AP iedere klacht als een handhavingsverzoek beschouwt onder de Awb, waarbij zij naar haar mening daarmee verplicht is in ieder verzoek een klacht te lezen en deze daarmee individueel af te doen.

De samenloop tussen privaatrecht en publiekrecht, als ook een nadere duiding van mogelijke klachten door de wetgever lijkt hier op zijn plaats.

Wie lost de klacht op? En is een opgeloste klacht echt opgelost? Kortom, wanneer is er voor een organisatie een bepaalde vorm van rechtszekerheid dat een mogelijke klacht voor en door niet oneindig veel privaat en publieke toezichthouders wordt behandeld, maar uit net iets andere invalshoek of eigen (niet afgestemde) normuitleg?

11. Rechtbank Rotterdam exclusief bevoegd

Afsluitend geldt ook dat de keuze voor het bevoegd verklaren van de rechtbank Rotterdam vragen oplevert. Wat betekent dit voor geschillen van gemengde aard, waarin zowel de AVG als de Dataverordening een rol spelen?

Dat soort gemengde geschillen lijken bepaald niet ondenkbaar, zeker gelet op de ruime definitie van het begrip “persoonsgegevens”. En competentieschillen treden dan al snel op; de consument kan op grond van de AVG immers per definitie in zijn eigen woonplaats terecht (artikel 79 lid 2 AVG).

12. Evaluatie

In de MvT is opgenomen dat ter uitvoering van hoofdstuk XI van de Dataverordening een evaluatie zal worden uitgevoerd op de in artikel 49 van de Dataverordening benoemde onderdelen.

Gezien de door ons geconstateerde zorgen omtrent samenloop in toezicht en toezichthouders, die mogelijk een effectieve gegevensuitwisseling in de weg staat, is ons advies om in de Uitvoeringswet op te nemen dat bij die evaluatie eveneens een beoordeling wordt opgenomen van de tot stand gekomen samenwerkingen tussen tenminste de AP en de ACM, als ook de samenwerking met sectorale toezichthouders en in het bijzonder door de AP geaccrediteerde toezichthoudende organen of door de ACM gecertificeerde geschillenbeslechtsorganen. Met name ten aanzien van de behandeling en afhandeling van klachten door consumenten (de datasubjecten en daarmee “betrokkenen” onder de AVG) en daarmee een evaluatie van 1) de bescherming die consumenten hebben kunnen verkrijgen door een goede samenwerking en 2) hoe de samenwerking heeft bijgedragen aan de rechtszekerheid voor bedrijven en organisaties met betrekking tot de mogelijkheid van gegevensuitwisseling onder de Dataverordening.

13. Conclusie

Burger beschermd? Rechtszekerheid?

De VIRA voorziet problemen in de uitvoering van de Dataverordening door een samenloop in wetgeving in met name de AVG en daarmee in toezicht en handhaving door zowel de AP als de ACM. Die zorgen zijn groot en de VIRA vraagt zich daarom af waarom er niet is gekozen voor één toezichthouder voor data, die toezicht houdt op zowel de AVG als de Dataverordening, waarbij een privaat fundament van zelfregulering of sectortoezicht een eerste basis kan vormen.

Die enige uiteindelijke toezichthouder kan met één mond spreken en kan gelijke overtredingen in gelijke gevallen op gelijke wijze sanctioneren. Dit zorgt voor één uiteindelijke effectieve toezichthouder die één loket vormt waar betrokkenen c.q. datasubjecten zich toe kunnen wenden. Hiermee wordt fragmentatie voorkomen, en worden de rechtsgelijkheid en rechtszekerheid gewaarborgd.



Over VIRA

VIRA is de vereniging van gespecialiseerde advocaten op het gebied van data, AI, IT en recht. De vereniging is door de Nederlandse Orde van Advocaten erkend als specialisatievereniging.

De vereniging kent ca. 100 leden. Het doel van de vereniging is om kennis te delen, tussen leden onderling en ook met organisaties en instanties die een (belangrijke) rol spelen op het gebied van data, AI, IT en recht.

Contact over deze reactie

Mocht u naar aanleiding van deze reactie vragen hebben, dan zijn wij graag bereid nadere toelichting te geven. Wij zijn te bereiken via secretaris@vira.nl

VIRA