Artikel

Internationale doorgifte van persoonsgegevens: aandachtspunten bij het gebruik van modelcontracten

mr. D.S. de Boer*

1. Inleiding

In de Algemene verordening gegevensbescherming (AVG) zijn de beginselen en voorwaarden voor de verwerking van persoonsgegevens neergelegd.[1] Een van de voorwaarden is dat persoonsgegevens slechts binnen de Europese Economische Ruimte (EER) verwerkt mogen worden tenzij in landen buiten de EER ('derde landen') een vergelijkbaar passend beschermingsniveau kan worden geboden als binnen de EER.[2] Een van de instrumenten die ingezet kunnen worden om een passend beschermingsniveau in derde landen te bieden, zijn de modelcontracten. In juni 2021 heeft de Europese Commissie een nieuwe set modelcontracten gepubliceerd.[3] De nieuwe modelcontracten zouden een grondslag moeten bieden voor de doorgifte van persoonsgegevens naar derde landen. Het is echter de vraag hoe stevig die grondslag is, gelet op het Schrems II-arrest.[4] In dat arrest oordeelde het Europese Hof van Justitie dat het gebruik van modelcontracten niet in alle gevallen volstaat om persoonsgegevens in derde landen te mogen verwerken. Als gevolg van dit arrest is de grondslag voor de doorgifte van persoonsgegevens op basis van modelcontracten gaan wankelen.

Het doel van dit artikel is het signaleren van aandachtspunten bij het gebruik van modelcontracten, waarbij ik inzoom op de in 2021 gepubliceerde nieuwe modelcontracten en de gevolgen van het Schrems II-arrest. De opbouw van mijn bijdrage ziet er als volgt uit. In paragraaf 2 bespreek ik het wettelijk kader waarbinnen modelcontracten worden gebruikt. Vervolgens bespreek ik in paragraaf 3 de rolverdeling van partijen bij het gebruik van modelcontracten. Ik sta specifiek bij dit onderwerp stil omdat de rolverdeling tussen partijen bepalend is voor de verantwoordelijkheden en verplichtingen bij het gebruik van modelcontracten. In paragraaf 4 bespreek ik kort de verschillende grondslagen, waaronder modelcontracten, op basis waarvan persoonsgegevens in derde landen verwerkt mogen worden. Vervolgens beoordeel ik in paragraaf 5 in hoeverre de nieuwe modelcontracten (standaardcontractbepalingen) verschillen ten opzichte van de oude modelcontracten (modelcontractbepalingen). Daarbij staat de vraag centraal of en in hoeverre de wijzigingen gevolgen hebben voor de verantwoordelijkheden en verplichtingen van contractspartijen die gebruikmaken van de modelcontracten. Tot slot bespreek ik in paragraaf 6 de invloed van het Schrems II-arrest op het gebruik van modelcontracten.

* Mr. D.S. de Boer is advocaat bij Dirkzwager legal & tax te Arnhem.

1 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming).

2 De AVG is van toepassing op landen die onderdeel zijn van de EER. De EER bestaat uit de EU-lidstaten en Liechtenstein, Noorwegen en IJsland.

3 Op grond van art. 46 lid 1 sub c worden de modelcontracten door de Europese Commissie vastgesteld. De vaststelling van de modelcontracten vindt plaats volgens een onderzoeksprocedure waarbij de Europese Commissie wordt bijgestaan door een comité in de zin van Verordening (EU) 182/2011.

4 Hof van Justitie 16 juli 2020, ECLI:EU:C:2020:559 (Schrems II).

doi: 10.5553/Contr/156608932021023004002

2. Wettelijk kader: doorgifte van persoonsgegevens

Modelcontracten hebben tot doel een grondslag te bieden voor doorgifte van persoonsgegevens naar derde landen. Om te kunnen bepalen of (überhaupt) sprake is van een doorgifte van persoonsgegevens naar derde landen moet naar het wettelijk kader van de modelcontracten worden gekeken. In deze paragraaf bespreek ik in enkele stappen het wettelijk kader waarbinnen de modelcontracten zich bevinden.

De AVG is, in de kern, van toepassing op zowel analoge als digitale verwerkingen van persoonsgegevens.[5] Wil men kunnen spreken van analoge verwerking, dan moeten gegevens op een enigszins gestructureerde wijze in een bestand zijn opgenomen.[6] Persoonsgegevens zijn (een combinatie van) gegevens die direct of indirect herleidbaar zijn tot een natuurlijk persoon ('de betrokkene'). Enkele voorbeelden van persoonsgegevens zijn naw-gegevens (naam, adres, woonplaats), telefoonnummers, e-mailadressen en IP-adressen.[7] Het is daarbij irrelevant of die gegevens zakelijk of privé van aard zijn. Met een 'verwerking' worden activiteiten bedoeld zoals het opslaan, bijwerken, wijzigen, versturen en verstrekken van persoonsgegevens. Als stelregel zou je kunnen zeggen dat een verwerking ieder werkwoord is dat je kunt plaatsen achter het woord persoonsgegevens. 'Doorgifte' is het doorgeven van persoonsgegevens van landen binnen de EER naar landen buiten de EER. Doorgifte van persoonsgegevens is dan ook een vorm van gegevensverwerking.

3. Rolverdeling partijen: verwerker en verwerkingsverantwoordelijke

Wanneer sprake is van een verwerking van persoonsgegevens, is het van belang vast te stellen vanuit welke rol partijen persoonsgegevens verwerken.[8] In deze paragraaf bespreek ik de algemene uitgangspunten van de rolverdeling en in paragraaf 4 ga ik nader in op de rolverdeling bij het gebruik van modelcontracten. Partijen kunnen persoonsgegevens verwerken vanuit de rol van verwerkingsverantwoordelijke of verwerker. Indien een partij de controle en beschikking heeft over persoonsgegevens en het doel en middel van de verwerking hiervan bepaalt, handelt die partij als verwerkingsverantwoordelijke.[9] Indien een partij van een verwerkingsverantwoordelijke de opdracht krijgt om binnen gegeven instructies persoonsgegevens te verwerken, handelt die partij als verwerker.[10] Een verwerker verwerkt dus slechts op instructie en ten behoeve van de verwerkingsverantwoordelijke en mag persoonsgegevens niet voor eigen doeleinden verwerken. Dit leidt ertoe dat de rol van een partij onder de AVG wordt bepaald door de feitelijke situatie en niet door de formele kwalificatie. De European Data Protection Board (EDPB)[11] stelt dat de begrippen verwerker en verwerkingsverantwoordelijke, als bedoeld in de AVG, functionele begrippen zijn en schrijft hierover het volgende:

> 'The concepts of controller and processor are functional concepts: they aim to allocate responsibilities according to the actual roles of the parties. This implies that the legal status of an actor as either a 'controller' or a 'processor' must in principle be determined by its actual activities in a specific situation, rather than upon the formal designation of an actor as being either a 'controller' or 'processor' (e.g. in a contract)'.[12]

Gelet op de functionele aard van de begrippen verwerker en verwerkingsverantwoordelijke is het aan te raden om afspraken over de taken en bevoegdheden van partijen op een duidelijke wijze in een overeenkomst op te nemen. Dit kan in de hoofdovereenkomst worden geregeld of in het geval van een verwerker-verwerkingsverantwoordelijke relatie in de verwerkersovereenkomst. Het sluiten van een verwerkersovereenkomst is bij de verwerker-verwerkingsverantwoordelijke relatie verplicht.[13]

Het is overigens niet zo dat bij een overeenkomst tussen twee partijen een standaard rolverdeling bestaat, waarbij één partij de verwerker is en de andere partij de verwerkingsverantwoordelijke is. Er zijn meerdere smaken mogelijk. Ik licht de verschillende smaken hierna kort toe.

De meest bekende smaak is de verwerkingsverantwoordelijke ↔ verwerker. Denk hierbij aan een IT-leverancier die in opdracht en ten behoeve van een bedrijf een hrm-systeem levert.[14] De IT-leverancier is in dit geval de verwerker. De IT-leverancier mag slechts ten behoeve en

5 Art. 2 AVG. Er gelden enkele, beperkte, uitzonderingen op het materieel toepassingsgebied die ik in dit artikel onbesproken laat.

6 Hof van Justitie 10 juli 2018, ECLI:EU:C:2018:551 (Jehovan todistajat).

7 Hof van Justitie 19 oktober 2016, ECLI:EU:C:2016:779 (Breyer).

8 Zie voor een nadere toelichting European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 1.0, 20 september 2020.

9 Art. 4 sub 7 AVG; zie ook European Data Protection Board 20 september 2020, p. 9 e.v.

10 Art. 4 sub 8 AVG; zie ook European Data Protection Board 20 september 2020, p. 24 e.v.

11 De European Data Protection Board is een onafhankelijk Europees orgaan dat bestaat uit vertegenwoordigers van Europese nationale toezichthoudende autoriteiten die belast zijn met het toezicht op naleving van de AVG. De European Data Protection Board is bevoegd om onder andere (niet-bindende) aanwijzingen te geven, richtlijnen op te stellen en aanbevelingen te doen.

12 European Data Protection Board 20 september 2020, p. 9 e.v.

13 Art. 28 AVG.

14 Een Human Resource Management systeem ('HRM-systeem') is een systeem waarin de personeelsadministratie van een bedrijf kan worden geautomatiseerd. In het HRM-systeem kunnen gegevens van medewerkers worden verwerkt over onder andere indiensttreding, verlof, ziekte en salaris.

doi: 10.5553/Contr/156608932021023004002

in opdracht van het bedrijf persoonsgegevens van medewerkers van het bedrijf in het hrm-systeem verwerken. Het bedrijf is de verwerkingsverantwoordelijke omdat het bedrijf het doel en middel van de verwerking bepaalt, namelijk het verwerken van persoonsgegevens van medewerkers in een systeem ten behoeve van de personeelsadministratie.
Een tweede smaak is verwerkingsverantwoordelijke ↔ verwerkingsverantwoordelijke. Een voorbeeld hiervan is het delen van persoonsgegevens van burgers tussen overheidsinstellingen, zoals tussen een gemeente en de Belastingdienst. Hier kan nog een tweedeling worden gemaakt tussen het geval waarin verwerkingsverantwoordelijken zelfstandig voor hun eigen gegevensverwerking verantwoordelijk zijn, en het geval waarin sprake is van een gezamenlijke verantwoordelijkheid.[15]
Tot slot is het ook mogelijk dat een verwerker een 'subverwerker' inschakelt.
Samengevat moeten partijen op grond van de AVG, voorafgaand aan de gegevensverwerking en op basis van feitelijke omstandigheden, bepalen wat de rolverdeling is en (in veel gevallen) deze rolverdeling met bijbehorende afspraken ook ergens vastleggen.

4. Passend beschermingsniveau bij doorgifte

4.1 Algemeen

Op grond van de AVG moet bij de verwerking van persoonsgegevens een passend beschermingsniveau worden gewaarborgd. Aangenomen wordt dat binnen de EER het passend beschermingsniveau gewaarborgd is (voor zover partijen zich aan de voorwaarden uit de AVG houden). Op het moment dat persoonsgegevens naar landen buiten de EER worden doorgegeven, valt de waarborg van het passend beschermingsniveau weg. Het territoriale toepassingsgebied van de AVG is immers in beginsel beperkt tot de EER.[16] Doordat het passend beschermingsniveau niet standaard kan worden gewaarborgd bij de doorgifte van persoonsgegevens naar landen buiten de EER, hebben partijen een (aanvullende) grondslag nodig om de persoonsgegevens te mogen doorgeven. Modelcontracten zijn een van de instrumenten die een grondslag bieden. In deze paragraaf bespreek ik in een notendop de verschillende instrumenten en zoom ik in op de modelcontracten.

4.2 Adequaatheidsbesluit

Op grond van artikel 45 AVG is het partijen toegestaan persoonsgegevens door te geven naar landen of gebieden die door de Europese Commissie zijn aangemerkt als 'veilige landen' en daarmee worden gekwalificeerd als landen met een passend beschermingsniveau. Op basis van een uitgebreide beoordeling die door de Europese Commissie wordt uitgevoerd, kan een land als zodanig worden aangemerkt. Bij een dergelijke beoordeling gaat de Europese Commissie niet over één nacht ijs. Het kan soms jaren duren voordat in een zogenoemd 'adequaatheidsbesluit' is vastgelegd dat een land een passend beschermingsniveau heeft en dat doorgifte naar het betreffende land wordt toegestaan. Op dit moment zijn er dertien landen buiten de EER waar op basis van een adequaatheidsbesluit persoonsgegevens verwerkt mogen worden.[17] Onder die landen bevindt zich het Verenigd Koninkrijk, dat afgelopen zomer aan de lijst is toegevoegd.[18]

4.3 Passende waarborgen

Artikel 46 AVG biedt een tweede mogelijkheid om persoonsgegevens door te geven naar derde landen. Deze mogelijkheid bestaat wanneer partijen bij de doorgifte van persoonsgegevens (1) passende waarborgen, (2) afdwingbare rechten en (3) doeltreffende rechtsmiddelen voor betrokkenen kunnen waarborgen. Artikel 46 lid 2 AVG geeft een limitatieve opsomming van instrumenten die ingezet kunnen worden om passende waarborgen te bieden. Dat betekent dat partijen naast het gebruik van een instrument uiteraard óók nog aan de voorwaarden van afdwingbare rechten en doeltreffende rechtsmiddelen moeten voldoen. Hier ga ik nader op in in paragraaf 6. Enkele van de instrumenten voor het bieden van passende waarborgen zijn: bindende bedrijfsvoorschriften ('binding corporate rules'),[19] goedgekeurde gedragscodes[20] en modelcontracten ('standard contractual clauses').[21] Ik beperk mij hier tot de modelcontracten en laat de andere instrumenten buiten beschouwing.
De modelcontracten zijn opgesteld door de Europese Commissie en bieden een grondslag voor de doorgifte van persoonsgegevens naar derde landen. In de modelcontracten is een aantal verantwoordelijkheden en verplichtingen neergelegd voor enerzijds de gegevensexporteur en anderzijds de gegevensimporteur.[22] De doorgifte begint in alle gevallen in landen binnen de EER. Dit betekent dat er sprake is van eenrichtingsverkeer. Het

15 Zie voor de definitie van gezamenlijke verantwoordelijke: European Data Protection Board 20 september 2020, p. 16 e.v.

16 Art. 3 AVG regelt het territoriale toepassingsgebied waarop de AVG van toepassing is. Het territoriale bereik van de AVG wordt grofweg beperkt tot (1) verwerkers en verwerkingsverantwoordelijken die in de EER zijn gevestigd en persoonsgegevens verwerken, en (2) partijen die niet in de EER zijn gevestigd, maar wel persoonsgegevens van EU-burgers verwerken. Met de vestiging van een partij wordt gedoeld op de locatie waar (economische) activiteiten worden uitgevoerd, ongeacht of in het kader van de vestiging de verwerking van persoonsgegevens plaatsvindt.

17 European Commission, Adequacy decisions, ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

18 European Commission, Decision on the adequate protection of personal data by the United Kingdom, 28 juni 2021, ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

19 Art. 46 lid 2 sub b jo. art. 47 AVG.

20 Art. 46 lid 2 sub e AVG.

21 Art. 46 lid 2 sub c AVG.

22 'Gegevensexporteur': partij die binnen de EER is gevestigd en persoonsgegevens doorgeeft naar de gegevensimporteur. 'Gegevensimporteur': partij die in een derde land is gevestigd en de persoonsgegevens ontvangt van de gegevensexporteur.

doi: 10.5553/Contr/156608932021023004002

belangrijkste kenmerk van de modelcontracten is dat contractspartijen op geen enkele wijze mogen afwijken van de bepalingen. De reden hiervoor is dat de afspraken in de modelcontracten een passend beschermingsniveau moeten bieden. Wanneer contractspartijen te pas en te onpas kunnen afwijken van de modelcontracten, kan het passende beschermingsniveau niet gewaarborgd worden. Contractspartijen hebben daarentegen wel de mogelijkheid om met behulp van vastgestelde bijlagen nadere invulling te geven aan de modelcontracten.

4.4 Specifieke situaties

Tot slot geeft artikel 49 AVG de mogelijkheid om in specifieke situaties persoonsgegevens door te geven aan partijen die in derde landen zijn gevestigd.[23] Persoonsgegevens mogen bijvoorbeeld worden doorgegeven wanneer de betrokkene uitdrukkelijk toestemming geeft voor de doorgifte.[24] Daarbij geldt dat de betrokkene voorafgaand aan de doorgifte ingelicht moet worden over de risico's van de doorgifte naar het derde land. Voor alle opgesomde situaties geldt dat ze 'specifiek' moeten zijn. Met 'specifiek' wordt gedoeld op het incidentele karakter en de duur van de doorgifte.[25] Het continu doorgeven van persoonsgegevens van klanten aan een moederbedrijf dat in een derde land is gevestigd, kan niet onder een van de specifieke situaties worden geschaard. Dat betreft immers een doorgifte van een grote groep betrokkenen die stelselmatig plaatsvindt.
Gelet op het voorgaande is de hoofdregel dat persoonsgegevens niet naar landen buiten de EER doorgegeven mogen worden. Doorgifte van persoonsgegevens naar derde landen is slechts toegestaan, indien een beroep kan worden gedaan op (1) een adequaatheidsbesluit of (2) passende waarborgen of (3) specifieke situaties. De door de Europese Commissie opgestelde modelcontracten kunnen onder de categorie 'passende waarborgen' worden geschaard.

5. Oude modelcontractbepalingen versus nieuwe standaardcontractbepalingen

5.1 Algemeen

Modelcontracten zijn een van de instrumenten voor de doorgifte van persoonsgegevens naar derde landen. In 2001 is de eerste set modelcontracten verschenen.[26] Zij zijn door de jaren heen op enkele punten gewijzigd en aangevuld.[27] Op 4 juni 2021 is een geheel nieuwe set modelcontracten in de plaats gekomen van de oude modelcontracten.[28] Zoals aangekondigd, beoordeel ik in deze paragraaf de belangrijkste wijzigingen tussen de oude modelcontracten ('modelcontractbepalingen') en de nieuwe modelcontracten ('standaardcontractbepalingen').[29] De wijzigingen die ik hier bespreek hebben mijns inziens de grootste gevolgen voor partijen die gebruikmaken van de modelcontracten. Separaat bespreek ik in paragraaf 6 de nieuwe, en mogelijk meest essentiële, bepaling over de Data Transfer Impact Assessment. Tot slot beschouw ik de oude versies van de modelcontractbepalingen als één versie en laat ik onderlinge verschillen buiten beschouwing.

5.2 Toepassingsbereik

Een van de opvallende – en meest positief ontvangen – wijzigingen is dat de standaardcontractbepalingen flexibeler kunnen worden toegepast. De modelcontractbepalingen voorzagen slechts voor twee situaties in een grondslag voor de doorgifte, te weten (1) verwerkingsverantwoordelijke in EU ◊ verwerkingsverantwoordelijke in een derde land, en (2) verwerkingsverantwoordelijke in EU ◊ verwerker in derde land. Dit beperkte toepassingsbereik had tot gevolg dat modelcontractbepalingen in veel gevallen onbruikbaar waren. In 2010 werd het probleem van het beperkte toepassingsbereik ook door de Working Party[30] aangekaart. De Working Party signaleerde dat er geen modelcontractbepalingen waren voor onder meer de situatie waarin de verwerker in de EU was gevestigd en de subverwerker in een derde land en deed vervolgens enkele suggesties.[31]

23 Art. 49 AVG.

24 Art. 49 lid 1 sub a AVG.

25 'Article 49 GDPR has an exceptional nature. The derogations it contains must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive.' European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10 november 2020, p. 14. Zie ook European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 mei 2018.

26 Beschikking van de Commissie van 15 juni 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen krachtens Richtlijn 95/46/EG.

27 Beschikking van de Commissie van 27 december 2004 tot wijziging van Beschikking 2001/497/EG betreffende de invoering van alternatieve modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen; Besluit van de Commissie van 5 februari 2010 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens aan in derde landen gevestigde verwerkers krachtens Richtlijn 95/46/EG van het Europees Parlement en de Raad.

28 Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 4 juni 2021 betreffende standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad ('Standaardcontractbepalingen').

29 Ten behoeve van de leesbaarheid beperk ik mij tot de definities uit de AVG en laat ik de definities uit de Richtlijn 95/46/EG inzake de verwerking van persoonsgegevens achterwege.

30 Article 29-Data Protection Working Party was een onafhankelijke Europese werkgroep die tot 25 mei 2018 verantwoordelijk was voor de behandeling van kwesties in verband met de bescherming van de persoonlijke levenssfeer en van persoonsgegevens en werd opgevolgd door de EDPB.

31 Article 29-Data Protection Working Party, FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, 00070/2010, p. 3, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp176_en.pdf.

doi: 10.5553/Contr/156608932021023004002

De standaardcontractbepalingen hebben deze leemte opgevuld door met vier modules te werken die van toepassing zijn op verschillende situaties. Het gaat om de volgende modules.

- module 1: gegevensexporteur en gegevensimporteur zijn verwerkingsverantwoordelijke;
- module 2: gegevensexporteur is een verwerkingsverantwoordelijke en gegevensimporteur een verwerker;
- module 3: gegevensexporteur en gegevensimporteur zijn verwerker;
- module 4: gegevensexporteur is een verwerker en gegevensimporteur een verwerkingsverantwoordelijke.

In de standaardcontractbepalingen wordt per module aangegeven aan welke voorwaarden partijen dienen te voldoen. Zo zijn de beginselen van doelbinding, transparantie en gegevensminimalisatie[32] opgenomen, en wordt vermeld welke voorwaarden er gelden voor het inschakelen van subverwerkers.[33] In wezen wordt zo door standaardcontractbepalingen de kern van de AVG als contractuele verplichting vastgelegd. Voor module 2 en 3 geldt bovendien dat er specifieke bepalingen zijn opgenomen die overeenkomen met afspraken uit de verwerkersovereenkomst.[34] Dit leidt ertoe dat partijen kunnen volstaan met de standaardcontractbepalingen en dat zij geen aanvullende verwerkersovereenkomst hoeven te sluiten. Tegelijkertijd kunnen partijen voor gegevensverwerking die alleen binnen de EER plaatsvindt er wel belang bij hebben om voor dat deel een aanvullende verwerkersovereenkomst te sluiten. Het voordeel van een dergelijke aanvullende verwerkersovereenkomst is dat partijen voor die verwerking afwijkende afspraken mogen opnemen over aansprakelijkheidsbepalingen, verantwoordelijkheden en verplichtingen en de afhandeling van datalekmeldingen.

5.3 Derdenbeding[35]

In de oude modelcontractbepalingen was een derdenbeding opgenomen ten behoeve van de betrokkene. Op grond van het derdenbeding kon de betrokkene een beperkt aantal rechten uitoefenen die uitdrukkelijk in de modelcontractbepalingen waren opgenomen. Bijvoorbeeld het recht op informatie over onder andere de gegevensimporteur en doorgifte van bijzondere persoonsgegevens, maar ook het recht op schadevergoeding en het recht om een geschil voor te leggen aan een gerechtelijke instantie, arbiter of mediator. Met het oog op het toebedelen van rechten aan derden zou het derdenbeding vergeleken kunnen worden met het derdenbeding in de zin van artikel 6:253 van het Burgerlijk Wetboek (BW). Tegelijkertijd zijn er ook wezenlijke verschillen. Waar partijen op grond van artikel 6:253 BW de mogelijkheid hebben om een derdenbeding tot aan het moment van aanvaarding te herroepen, is het derdenbeding in de modelcontractbepalingen in alle gevallen onherroepelijk.[36]

Onder de huidige standaardcontractbepalingen zijn de rechten van betrokkenen uitgebreid. De betrokkene wordt als derde-begunstigde aangemerkt en kan een beroep doen op een aantal afspraken uit de standaardcontractbepalingen. Het betreft niet slechts een beroep op het recht op informatie, maar ook een beroep op naleving van de standaardcontractbepalingen. Dit laatste is een interessant en potentieel vergaand recht van de betrokkene. Aangezien in de bepalingen de kernbeginselen uit de AVG contractueel zijn vastgelegd, komt aan de betrokkene daarmee min of meer een beroep op de AVG toe. In theorie zou een betrokkene de verwerkingsverantwoordelijke aansprakelijk kunnen stellen wanneer de betrokkene constateert dat persoonsgegevens langer dan noodzakelijk worden verwerkt zonder dat daarbij passende maatregelen worden genomen.[37] Even daargelaten in hoeverre de betrokkene ook daadwerkelijk kan aantonen dat hij door deze omstandigheid schade heeft geleden.

5.4 Aansprakelijkheid[38]

Op grond van de oude modelcontractbepalingen had de betrokkene het recht om van de gegevensexporteur schadevergoeding te ontvangen voor schade als gevolg van een schending van de verplichtingen van een van de partijen of van een subverwerker. De schadevergoeding was beperkt tot schendingen die onder het derdenbeding vielen.[39] De gegevensexporteur kon de gegevensimporteur en/of subverwerker vervolgens aanspreken en verhaal halen. Verder was de gegevensimporteur jegens de gegevensexporteur aansprakelijk voor de subverwerker. Deze aansprakelijkheid werd beperkt tot gedragingen van de subverwerker die onder de uitvoering van de verplichtingen van de subverwerker vielen.[40]

In de bijlage was tot slot een facultatieve bepaling opgenomen waarin partijen onderling een aansprakelijkheidsregeling konden treffen.

Deze opzet is in de standaardcontractbepalingen op de schop gegaan. De aansprakelijkheidsbepaling[41] is in twee opzichten in belangrijke mate gewijzigd ten opzichte van de modelcontractbepalingen. Ten eerste heeft de betrokkene de mogelijkheid om ieder van de partijen aansprakelijk te stellen voor schade. Dit betekent dat de gegevensexporteur niet meer het vaste aanspreekpunt voor de betrokkene is. Voor de gegevens-

32 Bepaling 8 Standaardcontractbepalingen.
33 Bepaling 9 Standaardcontractbepalingen.
34 Bepaling 8.9 van module 2 en module 3 Standaardcontractbepalingen.
35 Bepaling 3 Standaardcontractbepalingen.
36 Het herroepen van het derdenbeding kan op basis van art. 6:253 lid 2 BW. Partijen kunnen er overigens ook voor kiezen om op grond van art. 6:253 lid 4 BW een onherroepelijk derdenbeding om niet op te nemen. Verder geldt dat partijen op basis van art. 6:253 BW de keuze kunnen maken over het al dan niet opnemen van een derdenbeding. In het geval van de modelcontracten wordt deze keuze niet aan de partijen overgelaten, maar ligt het derdenbeding besloten in de modelcontracten. Gelet op de aard van de modelcontracten kunnen partijen hier niet van afwijken (zie ook par. 4.3).
37 Bepaling 8.4 Standaardcontractbepalingen.
38 Bepaling 12 Standaardcontractbepalingen.
39 Bepaling 6 Standaardcontractbepalingen.
40 Bepaling 11 lid 1 Standaardcontractbepalingen.
41 Bepaling 12 Standaardcontractbepalingen.

exporteur is dit een gunstige wijziging, omdat de betrokkene de gegevensimporteur nu ook rechtstreeks kan aanspreken. Daarnaast is in de bepaling opgenomen dat partijen aansprakelijk zijn voor schade die zij elkaar hebben berokkend. In de oude modelcontractbepalingen was deze bepaling nog als een facultatief onderdeel in de bijlage opgenomen. In standaardcontractbepalingen is deze bepaling opgenomen in bepaling 12 en daarmee een verplicht onderdeel van de overeenkomst geworden. Partijen mogen immers niet afwijken van de bepalingen uit de modelcontracten, omdat deze in een vaste vorm zijn gegoten (zie paragraaf 4.3). Met deze wijziging staat vast dat partijen elkaar aansprakelijk kunnen stellen voor schade. Onduidelijkheid bestaat nog over de vraag of het partijen is toegestaan om nadere afspraken te maken, zoals het overeenkomen van een aansprakelijkheidsbeperking. Het overeenkomen van een eventuele aansprakelijkheidsbeperking jegens elkaar laat onverlet dat partijen jegens de betrokkene volledig aansprakelijk blijven. Tot slot behoudt de betrokkene het recht om schadevergoeding te vorderen voor iedere schending van de standaardcontractbepalingen.

5.5 Toepasselijk recht en forumkeuze[42]

In de modelcontractbepalingen was opgenomen dat het recht van de lidstaat waar de gegevensexporteur was gevestigd van toepassing is. Het zou dus altijd gaan om het recht van een EU-lidstaat. Verder had de betrokkene de keuze om een geschil voor te leggen aan een onafhankelijke persoon of aan een rechterlijke instantie in de lidstaat waar de gegevensexporteur was gevestigd. Dit laatste was een opmerkelijke bepaling, omdat hiermee voorbij werd gegaan aan het recht van de betrokkene om een procedure in te stellen in de lidstaat waar de betrokkene woont.[43]

In afwijking van de modelcontractbepalingen is bij de standaardcontractbepalingen niet vastgelegd dat het recht van toepassing is waar de gegevensexporteur is gevestigd. Het staat partijen vrij om te bepalen welk recht zij van toepassing willen verklaren, mits dit het recht van een EU-lidstaat betreft én wordt voorzien in de rechten ten behoeve van derden. Waar de mogelijkheden voor toepasselijk recht zijn verbreed, zijn de mogelijkheden voor forumkeuze beperkt. Geschillen kunnen enkel worden beslecht door een gerecht. Het is niet meer mogelijk om een geschil bij een arbiter of mediator neer te leggen. Dit geldt niet alleen voor geschillen tussen enerzijds de betrokkene en anderzijds de partijen, maar ook voor geschillen tussen partijen onderling. Tot slot is aan de bepaling toegevoegd dat de betrokkene het recht heeft om een gerechtelijke procedure aanhangig te maken bij het gerecht van de EU-lidstaat waar hij zelf verblijft. Met deze laatste toevoeging is de 'fout' uit de modelcontractbepalingen gerepareerd.

5.6 Beveiligingsmaatregelen[44]

In de modelcontractbepalingen zijn slechts in beperkte mate afspraken opgenomen over te nemen beveiligingsmaatregelen door de gegevensexporteur en gegevensimporteur. Het komt erop neer dat de gegevensexporteur ervoor moet instaan dat de gegevensimporteur voldoende maatregelen neemt en de gegevensimporteur in een bijlage moet vermelden welke beveiligingsmaatregelen hij neemt. Met deze bepalingen worden de minimale (beveiligings)voorwaarden voor de doorgifte vastgelegd.

In de standaardcontractbepalingen zijn de beveiligingsmaatregelen nader uitgewerkt. Niet alleen is opgenomen dát partijen beveiligingsmaatregelen moeten nemen, maar ook op welke wijze dat moet worden gedaan. Zo wordt in bepaling 8 aangegeven dat partijen het gebruik van encryptie of het pseudonimiseren van persoonsgegevens in overweging moeten nemen, en dat de gegevensimporteur regelmatig controles moet uitvoeren om een passend beschermingsniveau te kunnen blijven bieden. Ook worden eisen gesteld aan het handelen door de gegevensimporteur bij het constateren van een datalek.[45] Indien de gegevensimporteur een verwerker is, moet hij de gegevensexporteur in kennis stellen van het datalek en daarbij informatie verstrekken over onder andere de aard van de inbreuk, categorieën persoonsgegevens, aantal personen en waarschijnlijke gevolgen.[46] Verder moeten partijen de vertrouwelijkheid mede waarborgen door slechts aan eigen medewerkers toegang te verschaffen tot de persoonsgegevens voor zover dat noodzakelijk is. Tot slot is het een aanrader om bijlage II van de standaardcontractbepalingen er eens bij te pakken, omdat daar een concrete opsomming wordt gegeven van beveiligingsmaatregelen die partijen, en met name de gegevensimporteur, kunnen nemen. Enkele voorbeelden die in de bijlage worden gegeven zijn: maatregelen om gegevenswissing te garanderen, maatregelen voor identificatie en autorisatie van gebruikers, maatregelen om systeemconfiguratie te beschermen, en procedures voor het beoordelen en evalueren van technische en organisatorische maatregelen.

5.7 Overige aandachtspunten

Naast voornoemde wijzigingen hebben er nog enige kleinere aanpassingen plaatsgevonden. Ik vermeld hier kort de meest noemenswaardige aanpassingen. Aan de modelcontractbepalingen is een nieuwe bepaling toegevoegd op basis waarvan de gegevensexporteur garandeert dat hij heeft onderzocht of de gegevensimporteur zou kunnen voldoen aan de afspraken.[47] Dit vormt een

42 Bepaling 17 en 18 Standaardcontractbepalingen.

43 Art. 79 lid 2 AVG: 'Een procedure tegen een verwerkingsverantwoordelijke of een verwerker wordt ingesteld bij de gerechten van de lidstaat waar de verwerkingsverantwoordelijke of de verwerker een vestiging heeft. *Een dergelijke procedure kan ook worden ingesteld bij de gerechten van de lidstaat waar de betrokkene gewoonlijk verblijft*, tenzij de verwerkingsverantwoordelijke of de verwerker een overheidsinstantie van een lidstaat is die optreedt in de uitoefening van het overheidsgezag.'

44 Bepaling 8.5 van module 1, bepaling 8.6 van module 2, bepaling 8.6 van module 3 en bepaling 8.2 van module 4 Standaardcontractbepalingen.

45 Met een datalek wordt een 'inbreuk in verband met persoonsgegevens' bedoeld zoals gedefinieerd in art. 4 sub 12 AVG.

46 Deze verplichting komt overeen met de verplichting van de verwerkingsverantwoordelijke bij het melden van een inbreuk bij de Autoriteit Persoonsgegevens zoals neergelegd in art. 33 lid 3 AVG.

47 Bepaling 8 Standaardcontractbepalingen.

doi: 10.5553/Contr/156608932021023004002

zorgplicht voor de gegevensexporteur. Het kan de gegevensexporteur worden aangerekend als hij met onbetrouwbare partijen in zee gaat. Verder hebben partijen op basis van de standaardcontractbepalingen een documentatieplicht,[48] heeft de betrokkene het recht verkregen om bezwaar te maken tegen geautomatiseerde besluitvorming, waaronder profilering,[49] zijn er aanvullende verplichtingen opgenomen voor subverwerkers,[50] en hebben toezichthouders een grotere rol gekregen bij de beoordeling en controle van partijen die standaardcontractbepalingen gebruiken.[51] Tot slot mogen partijen die reeds gebruikmaakten van de oude modelcontractbepalingen deze tot 27 december 2022 gebruiken. Vanaf 27 december 2022 moeten partijen overstappen naar de standaardcontractbepalingen, dan wel een ander instrument voor de doorgifte gebruiken.[52]

6. Let op: modelcontracten niet altijd voldoende

6.1 Algemeen

Voor het bieden van een passend beschermingsniveau moet sprake zijn van (1) passende waarborgen, (2) afdwingbare rechten voor betrokkenen, en (3) doeltreffende rechtsmiddelen voor betrokkenen.[53] In het Schrems II-arrest oordeelde het Europese Hof van Justitie (hierna: het Hof) dat modelcontracten passende waarborgen bieden, maar niet automatisch voorzien in afdwingbare rechten en doeltreffende rechtsmiddelen voor betrokkenen. Dat betekent dat partijen in sommige gevallen boven op de modelcontracten aanvullende maatregelen moeten nemen om een passend beschermingsniveau te kunnen waarborgen. In deze paragraaf bespreek ik de impact van het arrest op het gebruik van modelcontracten.

6.2 Het arrest Schrems II[54]

In het Schrems II-arrest stond de vraag centraal of bij de doorgifte van persoonsgegevens naar de Verenigde Staten een beschermingsniveau werd geboden dat in grote lijnen overeenkwam met het beschermingsniveau in de Europese Unie. In casu betrof het persoonsgegevens van Facebookgebruikers die vanaf de Ierse vestiging van Facebook naar de Verenigde Staten werden doorgegeven. De persoonsgegevens werden op basis van het Privacy Shield – een instrument dat toentertijd beschikbaar was – doorgegeven.[55]

Het Hof oordeelde dat bij de doorgifte van persoonsgegevens naar de Verenigde Staten niet kon worden voldaan aan alle voorwaarden voor het bieden van een passend beschermingsniveau. Ten eerste bleek dat Amerikaanse veiligheidsdiensten onbeperkte toegang hadden tot persoonsgegevens van betrokkenen die geen Amerikaans staatsburger waren. Aan het verschaffen van toegang aan de veiligheidsdiensten worden geenszins beperkingen gesteld of voorwaarden geboden. Ook vindt er geen enkel rechtelijk toezicht plaats waaronder de toegang tot de persoonsgegevens wordt geboden.[56] Daarnaast hebben betrokkenen geen toegang tot een onafhankelijk en onpartijdig gerecht om rechtsmiddelen te kunnen aanwenden met bijvoorbeeld als doel het recht op rectificatie en/of verwijdering van persoonsgegevens uit te oefenen.[57] Voorgaande leidt ertoe dat het Hof van oordeel is dat het Privacy Shield als instrument onvoldoende waarborgen biedt voor de doorgifte van persoonsgegevens naar de Verenigde Staten. Het Privacy Shield wordt dan ook ongeldig verklaard.

6.3 Gevolgen van Schrems II-arrest

Met het ongeldig verklaren van het Privacy Shield verdween van de ene op de andere dag de grondslag voor doorgifte van persoonsgegevens naar de Verenigde Staten. Maar dat niet alleen. Opvallend aan dit arrest is dat het Hof zich niet beperkt tot het Privacy Shield en de doorgifte naar de Verenigde Staten, maar zich uitspreekt over doorgifte naar derde landen in algemene zin. Door de uitspraak stond de algehele doorgifte naar derde landen op losse schroeven. Het beperken of voorkomen van toegang tot persoonsgegevens door nationale veiligheidsdiensten en het verzekeren van toegang tot een onafhankelijk gerecht zijn externe factoren. Partijen kunnen geen contractuele afspraken maken over dergelijke externe factoren. Dit leidt ertoe dat modelcontracten niet in alle gevallen in een passend beschermingsniveau kunnen voorzien. Daags na de publicatie van het Schrems II-arrest publiceerde de EDPB een FAQ-document over de gevolgen van het arrest voor de doorgifte van persoonsgegevens naar derde landen.[58] De EDPB was kort en duidelijk: er kwam geen overgangsperiode en doorgifte naar derde landen was mogelijk illegaal.[59]

48 Bepaling 8.5 module 1, bepaling 8.9 module 3, bepaling 8.9 module 3, bepaling 8.3 module 4 Standaardcontractbepalingen.
49 Bepaling 10 sub d module 1 Standaardcontractbepalingen.
50 Bepaling 9 Standaardcontractbepalingen.
51 Bepaling 13 Standaardcontractbepalingen.
52 Art. 4 Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 4 juni 2021 betreffende standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad.
53 Art. 46 AVG.
54 Hof van Justitie 16 juli 2020, ECLI:EU:C:2020:559 (Schrems II).
55 Het Privacy Shield is een overeenkomst die in 2016 tussen de Europese Unie en de Verenigde Staten werd gesloten. Bedrijven uit de Verenigde Staten konden zich op basis van het Privacy Shield laten certificeren en met het certificaat aantonen dat zij voldoende beveiligingsmaatregelen hadden genomen ter bescherming van persoonsgegevens. Het Privacy Shield is door het Hof van Justitie in het Schrems II-arrest ongeldig verklaard.
56 Hof van Justitie 16 juli 2020, ECLI:EU:C:2020:559 (Schrems II), par. 183.
57 Hof van Justitie 16 juli 2020, ECLI:EU:C:2020:559 (Schrems II), par. 194.
58 European Data Protection Board, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 23 juli 2020.
59 European Data Protection Board 23 juli 2020, p. 3.

6.4 'Oplossing' is Data Transfer Impact Assessment

In hetzelfde FAQ-document tracht de EDPB partijen enigszins tegemoet te komen en komt de EDPB met enkele aanbevelingen. Een van de aanbevelingen bestaat uit een risicobeoordeling. Partijen moeten zelf beoordelen of doorgifte van persoonsgegevens op basis van modelcontracten mogelijk blijft. Bij de beoordeling moet rekening worden gehouden met de omstandigheden van de doorgifte en eventuele aanvullende maatregelen die door partijen genomen kunnen worden.[60] De aanvullende maatregelen moeten in combinatie met de modelcontracten ervoor zorgen dat wetgeving uit derde landen geen afbreuk kan doen aan het passende beschermingsniveau.[61] In november 2020 publiceerde de EDPB een stappenplan waarin de aanbevelingen voor de risicobeoordeling zijn verwerkt.[62] Daarnaast geeft de EDPB in een tweede document invulling aan de aanvullende maatregelen die partijen kunnen nemen.[63]

Middels de nieuwe standaardcontractbepalingen, die mede naar aanleiding van het Schrems II-arrest zijn geschreven, is handen en voeten gegeven aan de risicobeoordeling.[64] De risicobeoordeling wordt sindsdien aangeduid als de Data Transfer Impact Assessment ('DTIA'). Partijen moeten de DTIA voorafgaand aan de doorgifte van persoonsgegevens uitvoeren. Dit betekent dat beide partijen een eigen verantwoordelijkheid hebben tot het doen van deze beoordeling. Als onderdeel van de DTIA moeten (1) de specifieke omstandigheden van de doorgifte, (2) de wetten en praktijken van het derde land, en (3) de relevante contractuele, technische of organisatorische waarborgen worden beoordeeld. Het maken van deze omvangrijke beoordeling brengt een zware last met zich. In mijn advocatenpraktijk constateer ik dat het met name ingewikkeld is als het gaat om de beoordeling van de wetten en praktijken in derde landen. Partijen moeten stapels wetten en regelingen beoordelen en vervolgens concluderen waarom zij van mening zijn dat de wet- en regelgeving in een derde land wel/niet afbreuk doet aan het passende beschermingsniveau. Ter vergelijking: de Europese Commissie heeft een aantal jaren nodig om een (gelijksoortige) beoordeling te maken in het kader van een adequaatheidsbesluit. Hoe kan van private partijen worden verwacht dat zij naast hun bedrijfsvoering 'even' een DTIA doen, als de Europese Commissie de beoordeling niet eens binnen een jaar kan voltooien?

Gelet op het voorgaande ben ik van mening dat de DTIA-bepaling in de modelcontracten geen oplossing biedt voor het probleem van doorgifte naar derde landen. Partijen kunnen zich slechts verbinden tot het nakomen van contractuele afspraken. Zij hebben geen invloed op externe factoren, zoals op nationale veiligheidsdiensten die zichzelf (onbeperkte) toegang verschaffen tot persoonsgegevens. Het uitvoeren van een DTIA verandert daar niets aan.

Ondanks de omstandigheid dat de DTIA een schijnoplossing biedt, is het aan te raden om de DTIA waar nodig uit te voeren. De DTIA is een verplicht onderdeel van de modelovereenkomst en daarmee een voorwaarde voor de doorgifte van persoonsgegevens naar derde landen. Omdat het uitvoeren van een DTIA een verplicht onderdeel van de modelovereenkomst is, kan het achterwege laten daarvan mogelijk leiden tot een tekortkoming in de nakoming van de modelovereenkomst en dus leiden tot schadeplichtigheid (artikel 6:74 BW). Daarnaast bestaat het risico dat de Autoriteit Persoonsgegevens[65] handhavend optreedt wanneer zij constateert dat de DTIA niet is uitgevoerd en daarmee niet aan alle voorwaarden voor doorgifte wordt voldaan (zie paragraaf 6.5).

6.5 Handhaving

Zoals hiervoor besproken, gold er na de Schrems II-uitspraak geen overgangstermijn. Van partijen werd verwacht dat zij per direct maatregelen namen om bij de doorgifte een passend beschermingsniveau te bieden, dan wel de doorgifte naar derde landen te staken. Het lastige parket waarin partijen nog steeds zitten, weerhoudt nationale toezichthoudende autoriteiten er niet van om onderzoeken te verrichten en handhavend op te treden. Onder dit handhavend optreden kan het opleggen van boetes worden verstaan. De eerste boetes voor onrechtmatige doorgifte van persoonsgegevens naar derde landen zijn inmiddels opgelegd.[66] Op 27 september 2021 heeft de Noorse toezichthouder een boete opgelegd aan een bedrijf dat persoonsgegevens doorgaf aan een verwerker die in China was gevestigd. Uit onderzoek van de Noorse toezichthouder zou zijn gebleken dat het bedrijf onder meer geen verwerkersovereenkomst had gesloten, geen DTIA had verricht en geen grondslag had voor de doorgifte van persoonsgegevens naar China. Ook enkele andere nationale toezichthoudende autoriteiten hebben in het kader van doorgifte van persoonsgegevens naar derde landen handhavend opgetreden.[67] Zo ook de Portugese toezichthouder, die middels een besluit een partij heeft bevolen binnen 12 uur de doorgifte van persoonsgegevens naar de Verenigde Staten op te schorten.[68]

60 European Data Protection Board 23 juli 2020, par. 132-133.
61 European Data Protection Board 23 juli 2020, p. 3.
62 European Data Protection Board 10 november 2020. Op 18 juni 2021 is middels versie 2.0 een gewijzigde versie verschenen.
63 Zie voor aanbevelingen over aanvullende maatregelen European Data Protection Board 10 november 2020.
64 Bepaling 14 en 15 Standaardcontractbepalingen.
65 De Autoriteit Persoonsgegevens is de Nederlandse toezichthoudende autoriteit die toeziet op de naleving van de AVG.
66 European Data Protection Board, Spanish DPA Fines Vodafone Spain more than 8 Million Euros, 31 maart 2021. Aan Vodafone is een boete opgelegd van in totaal 8 miljoen euro voor vier verschillende overtredingen. Voor het doorgeven van persoonsgegevens naar derde landen zonder het waarborgen van een passend beschermingsniveau en daarmee het overtreden van art. 44 AVG is door de Spaanse toezichthoudende autoriteit een boete van 2 miljoen euro opgelegd; European Data Protection Board, The Norwegian Data Protection Authority: Ferde As fined, 13 oktober 2021.
67 Onder meer de toezichthoudende autoriteit van Beieren; zie hiervoor European Data Protection Board, Bavarian DPA (BayLDA) calls for German company to cease the use of 'Mailchimp' tool, 30 maart 2021.
68 European Data Protection Board, Portugeuse DPA (CNPD) suspended data flows to the USA, 28 april 2021.

doi: 10.5553/Contr/156608932021023004002

Mede gelet op het handhavingsrisico is het voor partijen van belang om zo goed en kwaad als het kan een passend beschermingsniveau te bieden bij doorgifte van persoonsgegevens. Partijen kunnen hierbij een zogenoemde drietrapsraket hanteren. De eerste, en meest voor de hand liggende stap, is om een passend beschermingsniveau te bieden door de persoonsgegevens binnen de EER te (laten) verwerken. Indien dat niet mogelijk is, kan als tweede stap onderzocht worden of persoonsgegevens op basis van een adequaatheidsbesluit in derde landen verwerkt kunnen worden. Doet deze mogelijkheid zich niet voor, dan zou als derde stap beoordeeld moeten worden of bij de verwerking van persoonsgegevens in derde landen passende waarborgen geboden kunnen worden, zoals door gebruikmaken van modelcontracten.

7. Conclusie

Het doel van het gebruik van modelcontracten is het bieden van passende waarborgen voor doorgifte van persoonsgegevens naar landen buiten de EER. Middels de modelcontracten komen partijen contractueel overeen dat zij zich zullen houden aan de beginselen en voorwaarden uit de AVG. In deze bijdrage heb ik geconstateerd dat met de inwerkingtreding van de nieuwe standaardcontractbepalingen de verantwoordelijkheden en verplichtingen van partijen in omvang zijn toegenomen. In wezen is de kern van de AVG als pocketboek in de nieuwe standaardcontractbepalingen opgenomen.

Daarnaast heb ik het probleem gesignaleerd dat met het gebruik van modelcontracten niet altijd een passend beschermingsniveau wordt geboden bij doorgifte van persoonsgegevens naar derde landen. De modelcontracten bieden geen waarborgen tegen externe factoren, zoals overheidsingrijpen. Het verrichten van een DTIA en het nemen van aanvullende maatregelen biedt ook geen oplossing voor het probleem. Externe factoren kunnen immers niet contractueel geregeld worden. Dat leidt ertoe dat partijen worden opgezadeld met een welhaast onmogelijke opdracht. Het is daarom wachten op een realistische oplossing.

doi: 10.5553/Contr/156608932021023004002