

Guidelines



Richtsnoeren 07/2022 voor certificering als doorgifte-instrument

Versie 2.0

Vastgesteld op 14 februari 2023

Translations proofread by EDPB Members.
This language version has not yet been proofread.

VERSIEGESCHIEDENIS

Versie 1.0	14 juni 2022	Vaststelling van de richtsnoeren voor openbare raadpleging
Versie 2.0	14 februari 2023	Vaststelling van de richtsnoeren na openbare raadpleging

SAMENVATTING

Op grond van artikel 46 van de algemene verordening gegevensbescherming (AVG) moeten gegevens-exporteurs passende waarborgen bieden voor de doorgifte van persoonsgegevens aan derde landen of internationale organisaties. Daarom worden in de AVG de verschillende passende waarborgen aangegeven die gegevens-exporteurs overeenkomstig artikel 46 kunnen gebruiken als kader voor de doorgifte aan derde landen, onder meer door certificering in te voeren als nieuw doorgiftemechanisme (artikel 42, lid 2, en artikel 46, lid 2, punt f), AVG).

Deze richtsnoeren vormen een leidraad voor de toepassing van artikel 46, lid 2, punt f), AVG over de doorgifte van persoonsgegevens aan derde landen of internationale organisaties op basis van certificering. Het document bestaat uit vier delen en een bijlage.

In het eerste deel van dit document (“ALGEMENE BEPALINGEN”) wordt toegelicht dat de richtsnoeren een aanvulling vormen op de reeds bestaande algemene Richtsnoeren 1/2018 voor certificering en wordt ingegaan op de specifieke vereisten uit hoofdstuk V van de AVG voor gevallen waarin certificering als doorgifte-instrument wordt gebruikt. Volgens artikel 44 AVG mogen persoonsgegevens slechts aan derde landen of internationale organisaties worden doorgegeven indien naast aan de bepalingen van hoofdstuk V van de AVG ook wordt voldaan aan de voorwaarden van de andere bepalingen van de AVG. Daarom moet in eerste instantie de naleving van de algemene bepalingen van de AVG worden gewaarborgd, en in tweede instantie de naleving van de bepalingen van hoofdstuk V van de AVG. De partijen die hierbij zijn betrokken en hun belangrijkste taken in dit verband worden beschreven, met bijzondere aandacht voor de rol van de te certificeren gegevensimporteur en van de gegevens-exporteur die deze certificering zal gebruiken als kader voor zijn doorgiften (aangezien de gegevens-exporteur verantwoordelijk blijft voor de naleving van de voorschriften voor gegevensverwerking). In dit verband kan de certificering ook aanvullende maatregelen voor doorgifte-instrumenten omvatten, om zo de naleving van het beschermingsniveau van persoonsgegevens in de EU te waarborgen. Deel 1 van de richtsnoeren bevat ook informatie over de procedure voor het verkrijgen van een als doorgifte-instrument te gebruiken certificering.

In het tweede deel van deze richtsnoeren (“UITVOERINGSRICHTSNOEREN VOOR ACCREDITATIE-EISEN”) wordt gememoreerd dat de accreditatie-eisen van een certificeringsorgaan kunnen worden gevonden in ISO 17065 en door interpretatie van de Richtsnoeren 4/2018 inzake de accreditatie van certificeringsorganen op grond van artikel 43 AVG en de bijlage bij die richtsnoeren, rekening houdend met hoofdstuk V. Met betrekking tot een doorgifte worden in deze richtsnoeren echter enkele van de accreditatie-eisen voor het certificeringsorgaan nader toegelicht.

In het derde deel van deze richtsnoeren (“SPECIFIEKE CERTIFICERINGSCRITERIA”) wordt informatie gegeven over de certificeringscriteria die reeds zijn opgenomen in Richtsnoeren 1/2018 en worden aanvullende specifieke criteria geformuleerd die zouden moeten worden verwerkt in een certificeringsmechanisme dat moet worden gebruikt als instrument voor doorgifte naar derde landen. Deze criteria hebben betrekking op de beoordeling van de wetgeving van het derde land, de algemene verplichtingen van importeurs en exporteurs, voorschriften voor verdere doorgifte, verhaal en handhaving, de procedure en handelwijze in situaties waarin nationale wetgeving en praktijken de nakoming beletten van toezeggingen die zijn gedaan in het kader van een certificering en verzoeken van autoriteiten van derde landen om toegang tot gegevens.

In het vierde deel van deze richtsnoeren (“GEBRUIK VAN BINDEnde EN AFDWINGBARE TOEZEGGINGEN”) worden de onderwerpen beschreven die moeten worden geregeld in de bindende en afdwingbare toezeggingen die door verwerkingsverantwoordelijken of verwerkers die niet onder de AVG vallen moeten worden gedaan om passende waarborgen te bieden voor gegevens die aan derde landen worden doorgegeven. In deze toezeggingen, die kunnen worden opgenomen in diverse instrumenten, waaronder overeenkomsten, moet meer in het bijzonder worden gegarandeerd dat de importeur geen reden heeft om aan te nemen dat de wetgeving en praktijken die in het derde land op de desbetreffende verwerking van toepassing zijn de nakoming beletten van zijn toezeggingen in het kader van de certificering, waaronder verplichtingen om persoonsgegevens te verstrekken of maatregelen die toegang van overheidsinstanties toestaan.

In de BIJLAGE bij deze richtsnoeren zijn enkele voorbeelden opgenomen van aanvullende maatregelen die aansluiten bij de maatregelen in bijlage II bij Aanbevelingen 01/2020 (Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen) in het kader van het gebruik van een certificering als doorgifte-instrument. De voorbeelden zijn bedoeld om de aandacht op kritieke situaties te vestigen.

INHOUD

Versiegeschiedenis	2
SAMENVATTING	3
1 ALGEMENE BEPALINGEN	6
1.1 Doel en toepassingsgebied.....	6
1.2 Algemene voorschriften voor internationale doorgifte	6
1.3 Welke partijen zijn bij certificering als instrument voor doorgifte betrokken en wat is hun rol?	8
1.4 Wat zijn het toepassingsgebied en het voorwerp van certificering als doorgifte-instrument? ...	9
1.5 Wat zou de rol van de exporteur moeten zijn bij het gebruik van certificering als doorgifte-instrument?	10
1.6 Wat is de procedure voor certificering als doorgifte-instrument?	11
2 UITVOERINGSRICHTSNOEREN VOOR DE ACCREDITATIE-EISEN	12
3 SPECIFIEKE CERTIFICERINGSCRITERIA	13
3.1 UITVOERINGSRICHTSNOEREN VOOR DE CERTIFICERINGSCRITERIA	13
3.2 AANVULLENDE SPECIFIEKE CERTIFICERINGSCRITERIA	14
1. Beoordeling van de wetgeving van het derde land.....	14
2. Algemene verplichtingen van exporteurs en importeurs	15
3. Voorschriften voor verdere doorgifte	15
4. Verhaal en handhaving.....	15
5. Procedure en handelwijze in situaties waarin nationale wetgeving de nakoming van in het kader van certificering gedane toezeggingen belet	16
6. Behandeling van verzoeken van autoriteiten van derde landen om toegang tot gegevens	16
7. Aanvullende waarborgen met betrekking tot de exporteur	16
4 GEBRUIK VAN BINDEDE EN AFDWINGBARE TOEZEGGINGEN	17
BIJLAGE	20
A. VOORBEELDEN VAN DOOR DE IMPORTEUR TE NEMEN AANVULLENDE MAATREGELEN INDIEN DE DOORGIFTE ONDER DE CERTIFICERING VALT	20
B. VOORBEELDEN VAN AANVULLENDE MAATREGELEN WANNEER DE DOORVOER NIET ONDER DE CERTIFICERING VALT EN DE EXPORTEUR ER ZORG VOOR MOET DRAGEN	21

Het Europees Comité voor gegevensbescherming

Gezien artikel 70, lid 1, punt e), van 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 (hierna “AVG” genoemd),

Gezien de EER-Overeenkomst en met name bijlage XI en Protocol 37, zoals gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018¹,

Gezien de artikelen 12 en 22 van zijn reglement van orde,

HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD

1 ALGEMENE BEPALINGEN

1.1 Doel en toepassingsgebied

1. Dit document is bedoeld als leidraad voor de toepassing van artikel 46, lid 2, punt f), AVG over de doorgifte van persoonsgegevens aan derde landen of aan internationale organisaties op basis van certificering. Het EDPB heeft reeds algemene informatie over certificering² en accreditatie³ in het kader van de AVG gepubliceerd. Deze nieuwe richtsnoeren hebben daarom alleen betrekking op de specifieke aspecten van certificering als doorgifte-instrument. Zij bevatten nadere aanwijzingen voor de toepassing van artikel 46, lid 2, punt f) en artikel 42, lid 2, AVG in de vorm van praktische richtsnoeren op dit gebied en aanvullingen op de reeds gepubliceerde richtsnoeren.
2. De EPDB zal de werking van deze richtsnoeren evalueren aan de hand van de ervaringen die in de praktijk met hun toepassing zijn opgedaan, en een nadere toelichting geven op de onderstaande onderwerpen, waaronder de functie van de certificeringsovereenkomst met betrekking tot de bindende en afdwingbare toezeggingen als bedoeld in artikel 46, lid 2, punt f), AVG.

1.2 Algemene voorschriften voor internationale doorgifte

3. Volgens artikel 44 AVG mogen persoonsgegevens slechts aan derde landen⁴ of internationale organisaties worden doorgegeven indien naast aan de bepalingen van hoofdstuk V van de AVG ook wordt voldaan aan de voorwaarden van de andere bepalingen van de AVG. Elke doorgifte moet dus onder meer voldoen aan de beginselen voor de verwerking van persoonsgegevens van artikel 5 AVG, rechtmatig zijn krachtens artikel 6 AVG, en voldoen aan artikel 9 AVG, als er sprake is van bijzondere categorieën van gegevens. Bijgevolg moet er een tweeledige test worden toegepast. In eerste instantie

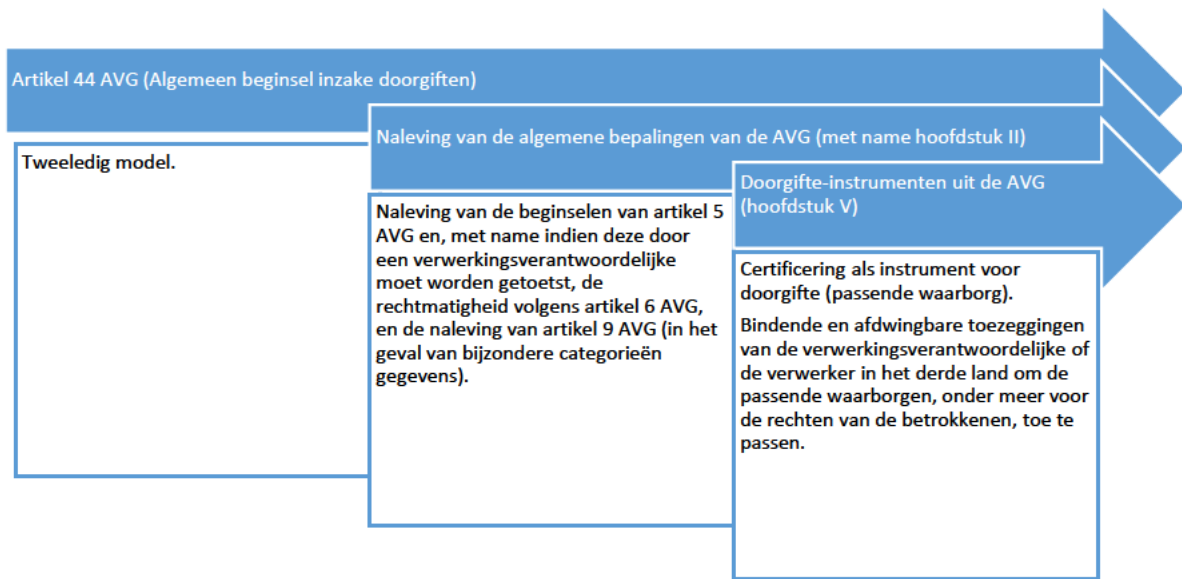
¹ Alle verwijzingen in dit document naar “lidstaten” moeten worden gelezen als verwijzingen naar “EER-lidstaten”.

² Richtsnoeren 1/2018 voor certificering en het vaststellen van certificeringscriteria overeenkomstig de artikelen 42 en 43 van de verordening.

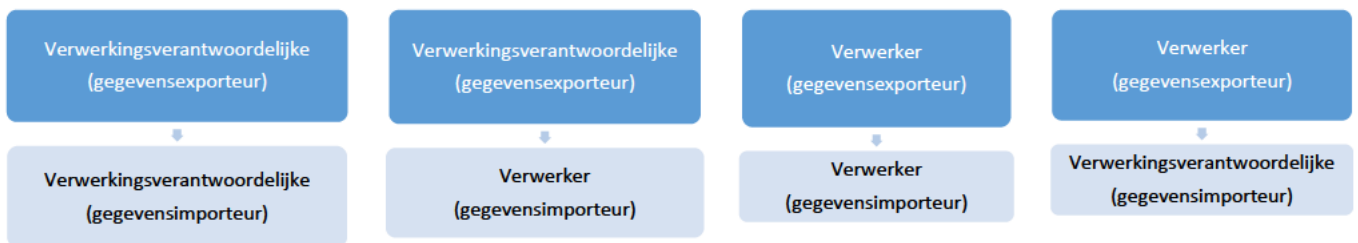
³ Richtsnoeren 4/2018 inzake de accreditatie van certificeringsorganen op grond van artikel 43 van de algemene verordening gegevensbescherming (2016/679).

⁴ Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (Richtsnoeren 05/2021 voor de wisselwerking tussen de toepassing van artikel 3 en de bepalingen over internationale doorgifte uit hoofdstuk V van de AVG), blz. 4.

moet de naleving van de algemene bepalingen van de AVG worden gewaarborgd, en in tweede instantie de naleving van de bepalingen van hoofdstuk V van de AVG.



4. In artikel 46 AVG wordt bepaald dat “[b]ij ontstentenis van een besluit uit hoofde van artikel 45, lid 3, [...] een doorgifte van persoonsgegevens aan een derde land of een internationale organisatie door een verwerkingsverantwoordelijke of een verwerker alleen [mag] plaatsvinden mits zij passende waarborgen bieden en betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken”. Krachtens artikel 46, lid 2, punt f), AVG kunnen die passende waarborgen worden geboden door middel van een goedgekeurd certificeringsmechanisme, samen met bindende en afdwingbare toezeggingen van de verwerkingsverantwoordelijke of de verwerker in het derde land om de passende waarborgen, onder meer voor de rechten van de betrokkenen, toe te passen.
5. De gegevensexporteur kan dus besluiten om door middel van de aan een gegevensimporteur toegekende certificering aan te tonen dat hij de verplichtingen naleeft die bijvoorbeeld voortvloeien uit artikel 24, lid 3, of artikel 28, lid 5, AVG. De gegevensimporteur kan besluiten om certificering aan te vragen om aan te tonen dat passende waarborgen worden geboden.
6. Zowel de gegevensexporteur als de gegevensimporteur kunnen verschillende rollen vervullen (bijvoorbeeld die van verwerkingsverantwoordelijke of verwerker)⁵, afhankelijk van de verwerking binnen hoofdstuk V, met verschillende verantwoordelijkheden tot gevolg:



7. Naast het gebruik van certificering of een van de andere instrumenten of mechanismen voor doorgifte als bedoeld in de artikelen 45 en 46 AVG, wordt in artikel 49 AVG bepaald dat in een beperkt aantal

⁵ Zie hieronder: UITVOERINGSRICHTSNOEREN VOOR DE CERTIFICERINGSCRITERIA.

specifieke situaties internationale doorgifte van gegevens kan plaatsvinden terwijl niet is voorzien in een ander in hoofdstuk V bedoeld mechanisme⁶. Zoals echter in eerdere richtsnoeren van het EDPB is aangegeven, moeten de afwijkingen waarin artikel 49 AVG, voorziet restrictief worden geïnterpreteerd, en houden zij voornamelijk verband met incidentele en niet-repetitieve verwerkingsactiviteiten⁷.

1.3 Welke partijen zijn bij certificering als instrument voor doorgifte betrokken en wat is hun rol?

8. Het **Europees Comité voor gegevensbescherming (EDPB)** is bevoegd om EER-brede certificeringscriteria goed te keuren (Europees gegevensbeschermingszegel) en om adviezen uit te brengen over ontwerpbesluiten van toezichthoudende autoriteiten over certificeringscriteria en accreditatie-eisen van de certificeringsorganen teneinde hun samenhang te waarborgen. Het EDPB is ook bevoegd om alle certificeringsmechanismen en gegevensbeschermingszegels en -merktekens in een register te verzamelen en openbaar te maken⁸.
9. De **toezichthoudende autoriteiten (TA's)** keuren de certificeringscriteria goed wanneer het certificeringsmechanisme geen Europees gegevensbeschermingszegel is⁹. Ook kunnen zij het certificeringsorgaan accrediteren, de certificeringscriteria opstellen en certificeringen afgeven indien het interne recht van hun lidstaat daarin voorziet¹⁰.
10. De **nationale accreditatie instantie** kan derde certificeringsorganen accrediteren op grond van ISO 17065 en de aanvullende accreditatie-eisen van TA's, die in overeenstemming zouden moeten zijn met deel 2 van deze richtsnoeren. In sommige lidstaten kan de accreditatie worden aangeboden door de bevoegde TA, maar ook worden uitgevoerd door een nationale accreditatie instantie, of door beide.
11. De eigenaar van een regeling is een identificeerbare organisatie die de certificeringscriteria en de vereisten aan de hand waarvan de conformiteit wordt beoordeeld, heeft opgesteld. De organisatie die de beoordelingen uitvoert, kan dezelfde organisatie zijn die ook het programma heeft ontwikkeld en eigenaar van de regeling is. Het kan echter zo zijn geregeld dat de ene organisatie de eigenaar van de regeling is, terwijl een of meer andere organisaties de beoordelingen uitvoeren.
12. Afhankelijk van het interne recht kan in plaats van de TA's bovengenoemd geaccrediteerd **certificeringsorgaan** de certificeringen afgeven¹¹. Het orgaan kan certificeringscriteria opstellen en dan dus eigenaar van de regeling zijn (zie punt 11). Het moet over een vestiging in de EER beschikken, met name om de in artikel 58, lid 2, punt f), AVG omschreven bevoegdheden tot het nemen van corrigerende maatregelen doeltreffend te kunnen uitoefenen. Het certificeringsorgaan kan echter werkzaam-

⁶ Voor nadere informatie over artikel 49 en de wisselwerking ervan met artikel 46 in het algemeen wordt verwezen naar Richtsnoeren 2/2018 inzake afwijkingen op grond van artikel 49 van Verordening 2016/679.

⁷ Richtsnoeren 2/2018 inzake afwijkingen op grond van artikel 49 van Verordening 2016/679, blz. 5.

Artikel 42, lid 8, AVG.

⁹ Richtsnoeren 1/2018 voor certificering en het vaststellen van certificeringscriteria overeenkomstig de artikelen 42 en 43 van Verordening (EU) 2016/679, punt 2.2.

Artikel 42, lid 5, en artikel 43, lid 1, GDPR.

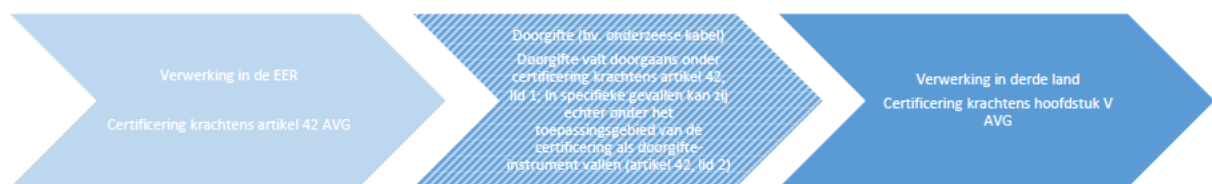
Artikel 42, lid 5, GDPR.

heden uitbesteden aan plaatselijke deskundigen of instellingen buiten de EER, die dan namens dit orgaan auditwerkzaamheden verrichten¹². Een certificeringsorgaan neemt echter altijd zelf het besluit over het al dan niet toekennen van een certificering.

13. De **gegevensimporteur** is de entiteit (verwerkingsverantwoordelijke of verwerker) in het derde land die van een gegevensexporteur gegevens ontvangt.
14. De **gegevensexporteur** is de entiteit (verwerkingsverantwoordelijke of verwerker) die vanuit de EER gegevens doorgeeft aan een gegevensimporteur. De gegevensexporteur moet de naleving van hoofdstuk V waarborgen.

1.4 Wat zijn het toepassingsgebied en het voorwerp van certificering als doorgifte-instrument?

15. Een certificeringsmechanisme als doorgifte-instrument uit hoofde van artikel 42, lid 2, moet zorgen voor passende waarborgen voor de verwerking van persoonsgegevens krachtens artikel 46, lid 2, punt f). Met de certificering moet het bestaan worden aangetoond van passende waarborgen die worden geboden door verwerkingsverantwoordelijken of verwerkers die buiten de EER zijn gevestigd of een internationale organisatie vormen en gegevens van verwerkingsverantwoordelijken of verwerkers uit de EER ontvangen, en bedoeld zijn om de specifieke risico's van de doorgifte van persoonsgegevens te beperken.
16. In algemene zin is de doorgifte van persoonsgegevens vanuit een lidstaat aan een derde land op zichzelf een verwerking van persoonsgegevens in de zin van artikel 4, lid 2, AVG, uitgevoerd in een lidstaat¹³, en dus certificeerbaar uit hoofde van artikel 42, lid 1, AVG. Afhankelijk van de situatie kan de doorgifte echter in sommige gevallen onder het toepassingsgebied van de certificering als doorgifte-instrument vallen. Daarom moet het voorwerp van de certificering — dat bij de certificering samenvalt met het onderwerp van beoordeling¹⁴ — in algemene zin de verwerking zijn van de gegevens die door de gegevensimporteur in het derde land vanuit de EER worden ontvangen, alsmede de doorgifte, indien deze onder toezicht van de importeur plaatsvindt.



17. Onder de certificering kan één enkele verwerking of een geheel van verwerkingen vallen. Daaronder kunnen governanceprocessen in de zin van organisatorische maatregelen zijn begrepen, dus als integraal onderdeel van een verwerking¹⁵.

¹² Certificeringsorganen beoordelen hun plaatselijke deskundigen overeenkomstig ISO 17065 en de aanvullende accreditatie-eisen die zijn vastgesteld door de toezichthoudende autoriteit (artikel 43, lid 1, punt b), AVG).

¹³ Arrest van het Hof van Justitie van de Europese Unie in zaak C-311/18, Data Protection Commissioner/Facebook Ireland Limited en Maximilian Schrems, punt 83.

¹⁴ Richtsnoeren 1/2018 voor certificering en het vaststellen van certificeringscriteria overeenkomstig de artikelen 42 en 43 van de verordening, blz. 18.

¹⁵ Richtsnoeren 1/2018 voor certificering en het vaststellen van certificeringscriteria overeenkomstig de artikelen 42 en 43 van de verordening, blz. 18 (bv. klachtenregeling).

18. De aanvragende entiteit zou derhalve de gegevensimporteur in het derde land zijn, voor zijn voorwerp van certificering.

1.5 Wat zou de rol van de exporteur moeten zijn bij het gebruik van certificering als doorgifte-instrument?

19. De doorgifte door de gegevensexporteur als zodanig valt in algemene zin rechtstreeks onder de AVG. De exporteur moet dus voldoen aan zijn verplichtingen uit hoofde van de AVG en meer in het bijzonder erop toezien dat gegevens overeenkomstig artikel 32 en hoofdstuk V veilig worden doorgegeven om ervoor te zorgen dat het door de AVG voor natuurlijke personen gewaarborgde beschermingsniveau niet wordt ondermijnd (artikel 44 AVG)¹⁶. Dit kan uiteraard worden gecertificeerd krachtens artikel 42, lid 1.
20. Verder is de gegevensexporteur die een certificering als passende waarborg in de zin van artikel 46, lid 2, punt f), AVG wil gebruiken met name verplicht om te verifiëren of de certificering die hij voornemens is te gebruiken doeltreffend is, gelet op de eigenschappen van de beoogde verwerking. Daartoe moet de gegevensexporteur de afgegeven certificering controleren, om na te gaan of het certificaat geldig en niet vervallen is, of het betrekking heeft op de specifieke uit te voeren doorgifte en of de doorgifte van persoonsgegevens onder het toepassingsgebied van de certificering valt, en tevens of van verdere doorgifte sprake is en of daaromtrent adequate documentatie is verstrekt. Bovendien moet de exporteur nagaan of het certificeringsorgaan dat de certificering afgeeft door een nationale accreditatie-instantie of een bevoegde toezichthoudende autoriteit is geaccrediteerd. Bovendien moet de gegevensexporteur in de in artikel 28 AVG, bedoelde gegevensverwerkingsovereenkomst vermelden dat certificering als doorgifte-instrument wordt gebruikt wanneer de doorgifte plaatsvindt van verwerkingsverantwoordelijke aan verwerker, of in een gegevensdelingsovereenkomst met de gegevensimporteur in geval van doorgifte van een verwerkingsverantwoordelijke aan een andere.
21. Aangezien de exporteur ervoor verantwoordelijk is dat alle bepalingen van hoofdstuk V worden toegepast, moet hij ook beoordelen of de certificering die hij voornemens is als doorgifte-instrument te gebruiken doeltreffend is, gelet op de geldende wetgeving en praktijken in het derde land die van toepassing zijn op de desbetreffende doorgifte. Ten behoeve van deze beoordeling, en als belangrijke manier om aan te tonen dat hij zijn verantwoordelijkheid nakomt, kan de gegevensexporteur gebruikmaken van de verificatie door het certificeringsorgaan van de gedocumenteerde beoordeling die de importeur opstelt van de wetten en praktijken van het derde land.
22. Indien uit de beoordeling van de importeur is gebleken dat deze en/of de gegevensexporteur op grond van de certificering mogelijk aanvullende maatregelen moet treffen om een in feite gelijkwaardig beschermingsniveau als in de EER te waarborgen, moet de gegevensexporteur de door de gecertificeerde

¹⁶ In dit verband moet worden opgemerkt dat artikel 44 AVG er duidelijk van uitgaat dat doorgifte niet alleen door een verwerkingsverantwoordelijke kan worden uitgevoerd, maar ook door een verwerker. Derhalve zal een doorgiftesituatie ontstaan waarin een verwerker gegevens naar een andere verwerker of zelfs naar een verwerkingsverantwoordelijke in een derde land zendt, op aanwijzing van zijn verwerkingsverantwoordelijke (artikel 28, lid 3, punt a), AVG). In deze gevallen treedt de verwerker namens de verwerkingsverantwoordelijke op als gegevensexporteur, en moet hij erop toezien dat de bepalingen van hoofdstuk V worden nageleefd voor de desbetreffende doorgifte, overeenkomstig de aanwijzingen van de verwerkingsverantwoordelijke, en dus ook dat een passend instrument voor doorgifte wordt gebruikt. Aangezien de doorgifte een verwerking is die namens de verwerkingsverantwoordelijke plaatsvindt, is de verwerkingsverantwoordelijke ook verantwoordelijk en mogelijk aansprakelijk overeenkomstig hoofdstuk V, en moet hij ervoor zorgen dat de verwerker voldoende garanties als bedoeld in artikel 28 biedt.

gegevensimporteur getroffen aanvullende maatregelen verifiëren en nagaan of hij in staat is de door de gegevensimporteur verlangde technische en (eventuele) aanvullende maatregelen te treffen.

23. Indien niet aan deze bepalingen wordt voldaan, moet de gegevensexporteur van de importeur verlangen dat deze aangepaste aanvullende maatregelen treft of deze zelf nemen.

1.6 Wat is de procedure voor certificering als doorgifte-instrument?

24. Certificering is vrijwillig, maar moet, indien zij wordt aangevraagd, worden toegekend middels een transparante procedure op basis van bindende voorschriften. De AVG stelt veel vertrouwen in private certificeringsmechanismen, als “gereguleerde zelfregulering”. Deze mechanismen moeten ook waarborgen dat de certificaten in materiële zin voldoen aan de vereisten voor de in artikel 46 AVG gedefinieerde passende waarborgen.
25. Daarom moet de certificering worden gebaseerd op de evaluatie van certificeringscriteria volgens een bindende auditmethodiek. Die criteria worden overeenkomstig artikel 42, lid 5, AVG goedgekeurd door de nationale TA's of door het EDPB. In de criteria voor certificering worden eisen opgenomen voor een beoordeling van de verwerking door de gegevensimporteur, met inbegrip van verdere doorgifte, en van het toepasselijke rechtskader van het derde land, om te voorkomen dat de voorschriften en praktijken van het derde land de importeur beletten zijn verplichtingen uit hoofde van de certificering na te komen.
26. Gedurende het certificeringsproces wordt het onderwerp van beoordeling aan de certificeringscriteria getoetst door een certificeringsorgaan dat is geaccrediteerd door de nationale accreditatie instantie of door de bevoegde TA¹⁷.
27. Volgens artikel 43, lid 1, AVG gaan certificeringsorganen die over de passende deskundigheid met betrekking tot gegevensbescherming beschikken, in voorkomend geval na kennisgeving aan de TA met het oog op de uitoefening van haar bevoegdheden overeenkomstig artikel 58, lid 2, punt h), AVG over tot afgifte en verlenging van het certificaat.
28. Volgens artikel 43, lid 5, AVG stellen de certificeringsorganen de bevoegde TA's in kennis van de redenen voor het afgeven of het intrekken van de aangevraagde certificering. Dit betekent niet dat het certificeringsorgaan de toestemming van de TA nodig heeft voor de afgifte van een certificering. Het certificeringsorgaan bewaakt de naleving door zijn cliënten van de certificeringscriteria.
29. De TA is bevoegd om als corrigerende maatregel een krachtens de artikelen 42 en 43 AVG, afgegeven certificering in te trekken of te doen intrekken, of om het certificeringsorgaan op te dragen geen certificering af te geven indien niet langer aan de vereisten voor de certificering wordt voldaan.
30. Een Europees gegevensbeschermingszegel voor internationale doorgiften van gegevens kan ook dienen als instrument voor doorgifte aan derde landen, in combinatie met bindende en afdwingbare toezeggingen¹⁸.

¹⁷ Richtsnoeren 4/2018 inzake de accreditatie van certificeringsorganen op grond van artikel 43 van de algemene verordening gegevensbescherming (2016/679), blz. 9.

¹⁸ Zie artikel 42, lid 5, AVG en punt 35 van Richtsnoeren 1/2018 van het EDPB voor certificering en het vaststellen van certificeringscriteria overeenkomstig de artikelen 42 en 43 van Verordening 2016/679.

31. Niettemin kunnen als doorgifte-instrument bedoelde certificeringen ook worden afgegeven overeenkomstig goedgekeurde nationale certificeringsregelingen van EER-lidstaten. Als zodanig zijn zij uitsluitend geldig voor doorgiften aan derde landen vanuit exporteurs in de EER-lidstaat waar de certificeringsregeling is goedgekeurd, aangezien er geen wederzijdse erkenning bestaat van certificeringen van verschillende EER-lidstaten. Het staat TA's in verschillende EER-lidstaten echter vrij om hetzelfde certificeringsmechanisme voor doorgifte goed te keuren¹⁹.

2 UITVOERINGSRICHTSNOEREN VOOR DE ACCREDITATIE-EISEN

32. De eisen voor accreditatie van een certificeringsorgaan voor certificeringen als doorgifte-instrument zijn te vinden in ISO 17065 en in een interpretatie van de Richtsnoeren 4/2018²⁰ tegen de achtergrond van hoofdstuk V, zoals hierna toegelicht.
33. Volgens het ingevolge artikel 64, lid 1, punt c), AVG uitgebrachte advies van het EDPB komen de aanvullende accreditatie-eisen die zijn opgesteld op basis van Richtsnoeren 4/2018 en ISO 17065 al overeen met de specifieke eisen die nodig zijn voor de accreditatie van een certificeringsorgaan ten aanzien van certificering als doorgifte-instrument. Voor situaties waarin doorgifte plaatsvindt, moeten voor sommige eisen de toelichting en de interpretatie echter nog nader worden uitgewerkt.
34. Ten aanzien van de benodigde middelen (zie eis 6 in bijlage 1 bij Richtsnoeren 4/2018) moet het certificeringsorgaan zorgen dat het beschikt over de benodigde middelen om te kunnen verifiëren of de importeur, zoals wordt voorgeschreven in de certificeringscriteria, de noodzakelijke beoordeling van de wetgeving en praktijken van het derde land of de derde landen waar hij is gevestigd of actief is naar behoren en juist heeft uitgevoerd²¹. Deze beoordeling zou voor de te certificeren verwerkingsactiviteiten moeten plaatsvinden als onderdeel van het voorwerp van de beoordeling met betrekking tot de passende waarborgen van artikel 46 AVG en omvat in voorkomend geval de door de importeur vastgestelde en uitgevoerde aanvullende maatregelen. Hieronder valt bijvoorbeeld ook ruime kennis van toepasselijke plaatselijke wetgeving en praktijken en voldoende taalvaardigheid voor het derde land of de derde landen.
35. Ten aanzien van de procesvereisten (zie eis 7 in bijlage 1 bij Richtsnoeren 4/2018) moet het certificeringsorgaan waarborgen dat het certificeringsproces kan worden ondersteund met eventuele audits ter plaatse, wordt uitgevoerd voor verwerkingen die zullen plaatsvinden in het derde land of de derde landen, en dat de beoordeling ook betrekking heeft op de praktische uitvoering van bestaande wetgeving en beleid in het derde land of de derde landen.

¹⁹ Indien een TA als eerste bepaalde certificeringscriteria in het kader van haar nationale initiatief goedkeurt, en vervolgens andere landen, rekening

houdend met de criteria van de regeling en de toepasselijke specifieke nationale voorschriften, eventueel dezelfde

certificeringscriteria willen vaststellen, kunnen zij dat doen zonder dat daarvoor een advies van het EDPB als bedoeld in artikel 64 AVG vereist is, en overeenkomstig artikel 64, lid 3, AVG gebruikmaken van het advies dat aan de eerste TA is uitgebracht (zie in dit verband Verwijzing naar richtsnoeren – Addendum (bijlage bij Richtsnoeren 1/2018 voor certificering en het vaststellen van certificeringscriteria overeenkomstig de artikelen 42 en 43 van de verordening), punt 66.

²⁰ Richtsnoeren 4/2018 inzake de accreditatie van certificeringsorganen op grond van artikel 43 van de AVG en de bijlage bij die verordening.

²¹ Zie punt 12 hiervoor.

36. Ten aanzien van de eisen met betrekking tot wijzigingen die van invloed zijn op de certificering (zie eis 7.10 in bijlage 1 bij Richtsnoeren 4/2018) moet het certificeringsorgaan wijzigingen in de wetgeving en/of de jurisprudentie van het derde land monitoren die van invloed kunnen zijn op de verwerking die onder het voorwerp van de beoordeling valt.

3 SPECIFIEKE CERTIFICERINGSCRITERIA

37. In het kader van de overweging van de specifieke certificeringscriteria zijn deze richtsnoeren gebaseerd op Richtsnoeren 1/2018 voor certificering en het vaststellen van certificeringscriteria overeenkomstig de artikelen 42 en 43 van de verordening (versie 3.0), de bijbehorende bijlage 2 over het herzien en beoordelen van certificeringscriteria overeenkomstig artikel 42, lid 5, en het addendum bij de richtsnoeren voor de beoordeling van certificeringscriteria.
38. Volgens het advies van het EDPB komen de certificeringscriteria die zijn opgesteld op basis van bijlage 2 bij Richtsnoeren 1/2018 en het addendum bij de richtsnoeren voor de beoordeling van certificeringscriteria al overeen met de meeste certificeringscriteria waarmee rekening moet worden gehouden bij het opstellen van een regeling voor certificering als doorgifte-instrument. Wellicht moeten echter enkele van deze bestaande criteria nader worden uitgewerkt om ze af te stemmen op een specifiek doorgiftescenario (zie punt 3.1). Daarnaast moeten wellicht aanvullende criteria worden geformuleerd met het oog op de toepassing van passende waarborgen, onder meer voor de rechten van betrokkenen (zie punt 3.2).

3.1 UITVOERINGSRICHTSNOEREN VOOR DE CERTIFICERINGSCRITERIA

39. Het toepassingsgebied van het certificeringsmechanisme en het onderwerp van beoordeling (zie bijlage 2, afdeling 2.a) moeten duidelijk worden omschreven in de desbetreffende documenten, ook voor de doorgifte van persoonsgegevens aan een derde land of de vraag of ook hun doorgifte onder het mechanisme moet vallen.
40. Ten aanzien van het toepassingsgebied van het certificeringsmechanisme en het onderwerp van beoordeling (zie bijlage 2, deel 2.b) moet in de desbetreffende documentatie concreet worden omschreven op welk type entiteit (bijvoorbeeld verwerkingsverantwoordelijke en/of verwerker) het certificeringsmechanisme van toepassing is.
41. Ten aanzien van het toepassingsgebied van het certificeringsmechanisme en het onderwerp van beoordeling (zie bijlage 2, deel 2.f) moet in de criteria worden voorgeschreven dat het onderwerp van beoordeling concreet wordt gedefinieerd om misverstanden te voorkomen. Die informatie moet ten minste het volgende omvatten:
42. de verwerking(en), ook wanneer verdere doorgiften worden overwogen;
- a) het doel;
 - b) het type entiteit (bv. verwerkingsverantwoordelijke en/of verwerker);
 - c) het type gegevens dat wordt doorgegeven, rekening houden met de vraag of dit bijzondere categorieën persoonsgegevens in de zin van artikel 9 AVG betreft;
 - d) de categorieën betrokkenen;
 - e) de landen waar de gegevensverwerking plaatsvindt.

43. Ten aanzien van transparantie en de rechten van betrokkenen (zie bijlage 2, punt 8) moet in de certificeringscriteria het volgende worden bepaald:
- a) aan betrokkenen moet informatie over de verwerkingsactiviteiten worden verstrekt, waaronder, indien relevant, informatie over de doorgifte van persoonsgegevens aan een derde land of een internationale organisatie (zie de artikelen 12, 13 en 14 AVG);
 - b) van betrokkenen moeten de rechten worden gewaarborgd op inzage, rectificatie, wissing, verwerkingsbeperking, kennisgeving inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking, alsmede het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit, in feite overeenkomend met de rechten als bedoeld in de artikelen 15 tot en met 19, 21 en 22 AVG;
 - c) een gecertificeerd gegevensimporteur moet een systeem voor klachtenbehandeling opzetten om doeltreffende handhaving van de rechten van betrokkenen te waarborgen;
 - d) beoordeeld moet worden of, en in hoeverre, deze rechten afdwingbaar zijn voor de betrokkenen in het desbetreffende derde land, en welke aanvullende passende maatregelen wellicht moeten worden genomen om die rechten te handhaven, bijvoorbeeld door voor te schrijven dat de importeur ermee instemt om zich te onderwerpen aan de rechtsmacht van, en om samen te werken met de toezichthoudende autoriteit die voor de exporteur(s) bevoegd is in procedures om de naleving van deze rechten te waarborgen en, in het bijzonder, dat hij ermee instemt om inlichtingen te verstrekken, audits te ondergaan en te voldoen aan de maatregelen die zijn vastgesteld door genoemde toezichthoudende autoriteit, waaronder corrigerende en compenserende maatregelen.
44. Ten aanzien van technische en organisatorische maatregelen die bescherming waarborgen (bijlage 2, punt 10.q) moet in de certificeringscriteria worden bepaald dat de importeur de exporteur op de hoogte moet brengen en, indien de importeur als verwerkingsverantwoordelijke optreedt, de voor de gegevensexporteur(s) bevoegde TA in de EER in kennis moet stellen van inbreuken in verband met persoonsgegevens en deze aan de betrokkenen moet mededelen indien de inbreuk waarschijnlijk een verhoogd risico inhoudt voor hun rechten en vrijheden, overeenkomstig de vereisten van artikel 34 AVG.

3.2 AANVULLENDE SPECIFIEKE CERTIFICERINGSKRITERIA

45. Gelet op de waarborgen die voor andere doorgifte-instrumenten zijn vastgesteld ingevolge artikel 46 AVG (waaronder bindende bedrijfsvoorschriften of gedragscodes) en om een consistent niveau van bescherming te waarborgen, en gelet op het Schrems II-arrest van het Hof, is het EDPB van mening dat in certificeringsmechanismen die als instrument voor doorgifte aan derde landen moeten worden gebruikt ook onderstaande criteria moeten worden opgenomen.

1. Beoordeling van de wetgeving van het derde land

- a) Wordt in de criteria bepaald dat de importeur een beoordeling moet hebben gemaakt van de voorschriften en praktijken van het derde land waar hij actief is, en van de vraag of zij de importeur beletten om zijn toezeggingen uit hoofde van de certificering na te komen?
- b) Wordt in de criteria bepaald dat de importeur de beoordeling van de voorschriften en praktijken van het derde land waar hij actief is moet documenteren en die documentatie beschikbaar moet houden voor het certificeringsorgaan en desgevraagd ook voor de in de EER voor de gegevensexporteur bevoegde TA en voor de gegevensexporteur?

- c) Wordt in de criteria bepaald dat de importeur de organisatorische en technische maatregelen moet opstellen en uitvoeren om de passende waarborgen van artikel 46 AVG te bieden, rekening houdend met Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen?
- d) Wordt in de criteria bepaald dat de importeur de organisatorische en technische maatregelen moet documenteren die daadwerkelijk zijn genomen om de passende waarborgen van artikel 46 AVG te bieden, en die documentatie beschikbaar moet houden voor het certificeringsorgaan en desgevraagd ook voor de bevoegde autoriteiten op het gebied van gegevensbescherming en voor de gegevensexporteur?
- e) Wordt in de criteria bepaald dat de importeur de organisatorische en technische maatregelen moet hebben opgesteld en uitgevoerd om de beveiliging van de doorgegeven persoonsgegevens te waarborgen, rekening houdend met de Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen indien de doorvoer onder het toepassingsgebied van de certificering als doorgifte-instrument valt?
- f) Wordt in de criteria bepaald dat aan het certificeringsorgaan en de exporteur moet worden gegarandeerd dat de importeur geen reden heeft om aan te nemen dat de op hem van toepassing zijnde wetgeving en praktijken hem kunnen beletten om zijn verplichtingen uit hoofde van de certificering na te komen?

2. Algemene verplichtingen van exporteurs en importeurs

- a) Wordt in de criteria bepaald dat in contractuele overeenkomsten (bijvoorbeeld in een bestaande dienstenovereenkomst) tussen exporteurs en importeurs een omschrijving moet worden opgenomen van de specifieke doorgifte waarop de certificering van toepassing is en dat aan de betrokkenen rechten ten behoeve van derden moeten worden toegekend?
- b) Voor zover in de criteria een specifieke inhoud voor deze contractuele overeenkomsten of instrumenten wordt voorgeschreven en een model wordt verstrekt, wordt in de criteria bepaald dat zij ook onder de evaluatie moeten vallen?

3. Voorschriften voor verdere doorgifte

- a) Wordt in de criteria bepaald dat op verdere doorgifte specifieke waarborgen van toepassing moeten zijn die aansluiten bij de vereisten in hoofdstuk V van de AVG, om te zorgen dat het in de EER gewaarborgde niveau van bescherming niet wordt ondermijnd, en wordt in de criteria bepaald dat passende documenten beschikbaar moeten worden gehouden voor het certificeringsorgaan en de in de EER voor de gegevensexporteur(s) bevoegde TA, en desgevraagd ook voor de gegevensexporteur?

4. Verhaal en handhaving

- a) Wordt in de criteria bepaald dat betrokkenen hun rechten als derde begunstigden jegens de gegevensimporteur moeten kunnen handhaven voor het gerecht van de gewone verblijfplaats van de betrokkene in de EER, of bij een internationale organisatie, ook voor vergoeding van schade die de betrokkene lijdt bij niet-naleving door de importeur van de toepasselijke certificeringsregeling?

- b) Is het op grond van de criteria mogelijk om adequaat te beoordelen of een importeur in de EER aansprakelijk is voor door de betrokkene geleden schade wanneer de toepasselijke certificeringsregeling niet wordt nageleefd?
- c) Wordt in de criteria bepaald dat betrokkenen een klacht tegen de importeur moeten kunnen indienen bij een toezichthoudende autoriteit in de EER, en met name in de EER-lidstaat van zijn of haar gewone verblijfplaats, plaats van werkzaamheid of de EER-lidstaat die voor de gegevensexporteur(s) bevoegd is?
- d) Wordt in de criteria bepaald dat de importeur moet samenwerken met de voor de gegevensexporteur(s) bevoegde toezichthoudende autoriteit in de EER en ermee moet instemmen dat hij door die autoriteit wordt geïnspecteerd, rekening moet houden met haar advies en haar beslissingen op moet volgen?

5. Procedure en handelwijze in situaties waarin nationale wetgeving de nakoming van in het kader van certificering gedane toezeggingen belet

- a) Wordt in de criteria, voor het geval dat de gegevensimporteur in een derde land of een internationale organisatie redenen heeft om aan te nemen dat wijzigingen in de toepasselijke wetgeving en praktijken hem kunnen beletten zijn verplichtingen uit hoofde van de certificering na te komen, bepaald dat deze gegevensimporteur het certificeringsorgaan en de gegevensexporteur daarvan onverwijld in kennis moet stellen, zodat deze laatste kan beoordelen of de doorgifte onmiddellijk moet worden gestaakt?
- b) Wordt in de criteria een omschrijving vereist van de te ondernemen stappen (waaronder kennisgeving aan de exporteur in de EER en het treffen van passende aanvullende maatregelen) voor het geval de gegevensimporteur wetgeving of praktijken van een derde land ter kennis komen die de naleving van verplichtingen uit hoofde van de certificering beletten, alsmede van de maatregelen die moeten worden genomen in geval van verzoeken om informatie van autoriteiten van derde landen (waaronder de verplichting om de rechtmatigheid van het verzoek te beoordelen en, indien nodig, aan te vechten, en om eventueel verstrekte informatie tot een minimum te beperken)?

6. Behandeling van verzoeken van autoriteiten van derde landen om toegang tot gegevens

- a) Wordt in de criteria bepaald dat de gegevensimporteur de gegevensexporteur onverwijld op de hoogte moet brengen van verzoeken van autoriteiten van derde landen om toegang, en passende aanvullende maatregelen moet nemen?
- b) Wordt in de criteria bepaald dat doorgifte naar aanleiding van oneigenlijke toegangsverzoeken van overheidsinstanties van derde landen, waaronder met name verzoeken die grootschalige en arbitraire doorgifte van persoonsgegevens behelzen, niet mag plaatsvinden?

7. Aanvullende waarborgen met betrekking tot de exporteur

46. Wordt in de criteria bepaald dat de gegevensimporteur in voorkomend geval, ook middels in dit opzicht voor de gegevensexporteur bindende vereisten, moet waarborgen dat aan de aanvullende maatregelen die hij heeft opgesteld overeenkomstige aanvullende maatregelen bij de gegevensexporteur worden verbonden, rekening houdend met Aanbevelingen 01/2020 van het EDPB en de praktijkvoorbeelden, om een doeltreffende uitvoering van de aanvullende maatregelen van de importeur te waarborgen?

4 GEBRUIK VAN BINDENDE EN AFDWINGBARE TOEZEGGINGEN

47. In artikel 42, lid 2, AVG wordt voorgeschreven dat niet onder de AVG vallende verwerkingsverantwoordelijken en verwerkers die zich bij een certificeringsmechanisme voor doorgiften hebben aangesloten tevens via contractuele of andere juridisch bindende instrumenten bindende en afdwingbare toezeggingen doen²² om de passende waarborgen toe te passen die door het certificeringsmechanisme worden geboden, ook wat betreft de rechten van betrokkenen.
48. Zoals aangegeven in de AVG, kunnen deze toezeggingen worden gedaan door middel van een overeenkomst, hetgeen de eenvoudigste oplossing lijkt te zijn. Er kunnen ook andere instrumenten worden gebruikt, op voorwaarde dat de verwerkingsverantwoordelijken/verwerkers die zich bij het certificeringsmechanisme hebben aangesloten de bindende en afdwingbare aard van die andere middelen kunnen aantonen.
49. In alle gevallen moet de bindende en afdwingbare aard worden gewaarborgd krachtens het recht van de EU en zouden de toezeggingen ook bindend en afdwingbaar moeten zijn door betrokkenen in de hoedanigheid van derde begunstigden.
50. Een eenvoudige optie zou zijn om de bindende en afdwingbare toezeggingen op te nemen in de overeenkomst tussen de gegevensexporteur en de gegevensimporteur. In de praktijk zouden de partijen een bestaande overeenkomst kunnen gebruiken (bijvoorbeeld een dienstenovereenkomst tussen de exporteur en de gegevensimporteur, de gegevensverwerkingsovereenkomst overeenkomstig artikel 28 AVG tussen verwerkingsverantwoordelijken en verwerkers, of een gegevensdelingsovereenkomst tussen afzonderlijke verwerkingsverantwoordelijken), waarin de bindende en afdwingbare toezeggingen zouden kunnen worden opgenomen. Deze toezeggingen zouden duidelijk moeten worden gescheiden van de overige bepalingen. Een andere optie is om te werken met een aparte overeenkomst, bijvoorbeeld door aan het certificeringsmechanisme voor doorgifte een modelovereenkomst toe te voegen die dan zou moeten worden ondertekend door verwerkingsverantwoordelijken/verwerkers in het derde land en al hun exporteurs.
51. Er moet ruimte zijn om de meest geschikte optie te kiezen, afhankelijk van de specifieke situatie.
52. Wanneer het certificeringsmechanisme bedoeld is voor gebruik voor doorgiften en verdere doorgiften door een verwerker aan subverwerkers, moet er ook in de verwerkingsovereenkomst tussen de verwerker en zijn verwerkingsverantwoordelijke worden verwezen naar het certificeringsmechanisme en het instrument dat voorziet in bindende en afdwingbare toezeggingen.

Voorbeeld van bindende en afdwingbare toezeggingen, opgenomen in de overeenkomst tussen gegevensexporteur en gegevensimporteur:

²² Dit juridisch bindende instrument mag geen ander hoofdstuk V-instrument zijn (waaronder, bijvoorbeeld, de standaardcontractbepalingen), aangezien deze in artikel 46, lid 2, punt f), bedoelde bindende en afdwingbare toezeggingen moeten zijn bedoeld om te zorgen dat de importeur de certificeringscriteria zal naleven.



53. In algemene zin moet in de overeenkomst of het andere juridisch bindende instrument worden bepaald dat de gecertificeerde verwerkingsverantwoordelijke/verwerker die als importeur optreedt, toezegt zich aan de voorschriften van de certificering voor doorgifte te zullen houden bij de verwerking van de desbetreffende uit de EER ontvangen gegevens, en garandeert geen reden te hebben om aan te nemen dat de op de desbetreffende verwerking van toepassing zijnde wetten en praktijken in het derde land, waaronder ook eventuele verplichtingen om persoonsgegevens te verstrekken of maatregelen die toegang door overheidsinstanties toestaan, hem beletten zijn toezeggingen uit hoofde van de certificering na te komen en dat hij de exporteur in kennis zal stellen van relevante wijzigingen in wetgeving of praktijken in dit verband.
54. De overeenkomst of het andere instrument moet ook voorzien in regelingen die deze toezeggingen afdwingbaar maken in geval van niet-naleving van de voorschriften van de certificering door de verwerkingsverantwoordelijke/verwerker die als importeur optreedt, met name wat betreft de rechten van betrokkenen van wie de gegevens op grond van de certificering worden doorgegeven.
55. Meer bepaald moet in de overeenkomst of het andere instrument het volgende worden geregeld:
- Betrokkenen van wie de gegevens krachtens de certificering worden doorgegeven, moeten het recht hebben om als derde begunstigen de toezeggingen van de gecertificeerde gegevensimporteur uit hoofde van de certificering af te dwingen.
 - Het punt van aansprakelijkheid in geval van schending van de voorschriften van de certificering door een gecertificeerde gegevensimporteur die buiten de EER gevestigd is. In het geval van een schending van de voorschriften van de certificering door een gecertificeerde gegevensimporteur die buiten de EER gevestigd is, moeten betrokkenen de mogelijkheid hebben om, door het inroepen van hun rechten ten behoeve van derden, tegen die entiteit een vordering in te stellen, ook tot schadevergoeding, bij een in de EER gevestigde toezichthoudende autoriteit en een rechterlijke instantie van het EER-land waar de betrokkene gewoonlijk verblijft. De gecertificeerde importeur moet de beslissing van de betrokkene om dit te doen eerbiedigen. Wanneer een schending door de importeur aansprakelijkheid van de gegevensexporteur tot gevolg kan hebben, moeten betrokkenen ook de mogelijkheid hebben om een vordering tegen de gegevensexporteur in te stellen bij de toezichthoudende autoriteit of de rechterlijke instantie van het land waar de

gegevensexporteur gevestigd is of waar de betrokkene gewoonlijk verblijft²³. De gegevensimporteur en de gegevensexporteur moeten ook aanvaarden dat de betrokkene door een orgaan, organisatie of vereniging zonder winstoogmerk kan worden vertegenwoordigd onder de voorwaarden van artikel 80, lid 1, AVG.

- De exporteur moet het recht hebben om ten aanzien van de gecertificeerde gegevensimporteur de voorschriften op grond van de certificering te handhaven als derde begunstigde.
- De gecertificeerde gegevensimporteur moet verplicht zijn om de exporteur en de toezichthoudende autoriteit van de gegevensexporteur in kennis te stellen van door het certificeringsorgaan genomen maatregelen naar aanleiding van een vastgestelde schending van de voorschriften van de certificering door dezelfde gegevensimporteur.

²³ Deze aansprakelijkheid moet onverminderd de mechanismen die op grond van de certificering kunnen worden uitgevoerd op het certificeringsorgaan rusten, dat overeenkomstig de certificering ook maatregelen tegen de gecertificeerde verwerkingsverantwoordelijken/verwerkers kan nemen door corrigerende maatregelen op te leggen.

BIJLAGE

A. VOORBEELDEN VAN DOOR DE IMPORTEUR TE NEMEN AANVULLENDE MAATREGELEN INDIEN DE DOORGIFTE ONDER DE CERTIFICERING VALT

Praktijkvoorbeeld 1: opslag van gegevens voor back-up- of andere doeleinden waarvoor geen toegang tot ongecodeerde gegevens is vereist

Er moeten criteria worden geformuleerd voor versleutelingsnormen en de beveiliging van de decoderingssleutel, waaronder met name criteria voor de juridische situatie in het derde land. Indien de importeur gedwongen kan worden om decoderingssleutels af te geven, kan de aanvullende maatregel niet als doeltreffend worden beschouwd²⁴.

Praktijkvoorbeeld 2: doorgifte van gepseudonimiseerde gegevens

In het geval van gepseudonimiseerde gegevens moeten criteria worden geformuleerd voor de beveiliging van de aanvullende informatie die nodig is om de doorgegeven gegevens te koppelen aan een geïdentificeerde of identificeerbare persoon, waaronder met name:

— Criteria voor de juridische situatie in het derde land. Indien de importeur gedwongen kan worden om aanvullende gegevens in te zien of te gebruiken om de gegevens aan een geïdentificeerde of identificeerbare persoon te koppelen, kan de maatregel niet als doeltreffend worden beschouwd²⁵.

— Criteria voor de definitie van aanvullende informatie die voor autoriteiten van derde landen beschikbaar is en kan volstaan om de gegevens aan een geïdentificeerde of identificeerbare persoon te koppelen.

Praktijkvoorbeeld 3: versleuteling van gegevens om deze te beschermen tegen toegang voor de overheidsinstanties van het derde land van de importeur tijdens de doorgifte tussen de exporteur en zijn importeur

In het geval van versleutelde gegevens moeten alle criteria voor de beveiliging van de doorvoer worden opgenomen. Indien de importeur kan worden gedwongen om cryptografische sleutels voor decoding of authenticatie af te geven, of om een voor doorvoer gebruikte component zodanig te wijzigen dat de beveiligingseigenschappen ervan worden ondermijnd, kan de aanvullende maatregel niet als doeltreffend worden beschouwd²⁶.

Praktijkvoorbeeld 4: beschermde ontvanger

In het geval van beschermde ontvangers, moeten criteria voor de grenzen van dit voorrecht worden geformuleerd. De gegevensverwerking moet binnen de grenzen van het verschoningsrecht blijven. Dit

²⁴ Bijlage 2, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, versie 2.0 (hierna "Aanbevelingen" genoemd), praktijkvoorbeeld 1: Opslag van gegevens voor back-up- of andere doeleinden waarvoor geen toegang tot ongecodeerde gegevens is vereist, punt 84; https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf

²⁵ Zie de Aanbevelingen, punten 85 tot en met 89.

²⁶ Zie de Aanbevelingen, punt 90.

geldt ook voor verwerking door (sub)verwerkers en verdere doorgifte, waarvan de ontvangers ook beschermd moeten zijn²⁷.

B. VOORBEELDEN VAN AANVULLENDE MAATREGELEN WANNEER DE DOORVOER NIET ONDER DE CERTIFICERING VALT EN DE EXPORTEUR ER ZORG VOOR MOET DRAGEN

Praktijkvoorbeeld 2: doorgifte van gepseudonimiseerde gegevens

Er moeten criteria worden geformuleerd voor de aanvullende informatie die voor de autoriteiten van het derde land beschikbaar is en kan volstaan om de gegevens aan een geïdentificeerde of identificeerbare persoon te koppelen.

Praktijkvoorbeeld 3: versleuteling van gegevens om deze te beschermen tegen toegang voor de overheidsinstanties van het derde land van de importeur tijdens de doorgifte tussen de exporteur en zijn importeur

Er moeten criteria worden geformuleerd voor de betrouwbaarheid van de certificeringsinstantie voor de publieke sleutel of de gebruikte infrastructuur, de beveiliging van de voor authenticatie of decodering gebruikte cryptografische sleutels en de betrouwbaarheid van het sleutelbeheer, en het gebruik van naar behoren onderhouden software zonder bekende kwetsbaarheden.

Indien de importeur kan worden gedwongen om voor decodering of authenticatie geschikte cryptografische sleutels te verstrekken, of om een voor doorvoer gebruikte component te wijzigen om de beveiligingseigenschappen ervan te ondermijnen, kan de aanvullende maatregel niet als doeltreffend worden beschouwd²⁸.

Praktijkvoorbeeld 4: beschermde ontvanger

In het geval van beschermde ontvangers, moeten criteria voor de grenzen van dit voorrecht worden geformuleerd. De gegevensverwerking moet binnen de grenzen van het verschoningsrecht blijven. Dit geldt ook voor verwerking door (sub)verwerkers en verdere doorgifte, waarvan de ontvangers ook beschermd moeten zijn²⁹.

²⁷ Zie de Aanbevelingen, punt 91.

²⁸ Zie de Aanbevelingen, punt 90.

²⁹ Zie de Aanbevelingen, punt 91.