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

Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen

Vastgesteld op 10 november 2020

Samenvatting

De Algemene Verordening Gegevensbescherming (AVG) van de Unie is aangenomen met een tweeledig doel: het vergemakkelijken van het vrije verkeer van persoonsgegevens binnen de Europese Unie en het handhaven van de grondrechten en vrijheden van personen, in het bijzonder het recht op bescherming van persoonsgegevens.

In het recente arrest in de zaak C-311/18 (Schrems II) wordt door het Hof van Justitie van de Europese Unie (HvJ-EU) in herinnering gebracht dat de in de Europese Economische Ruimte (EER) geboden bescherming van persoonsgegevens ook moet worden geboden als de gegevens naar elders worden doorgegeven. De doorgifte van persoonsgegevens naar derde landen mag geen middel zijn om de in de EER geboden bescherming te ondermijnen of af te zwakken. Het Hof bevestigt dit ook door toe te lichten dat het beschermingsniveau in derde landen niet identiek hoeft te zijn aan het in de EER gewaarborgde niveau, maar wel in grote lijnen hiermee moet overeenstemmen. Het Hof bevestigt tevens de geldigheid van standaardcontractbepalingen, als een doorgifte-instrument dat kan dienen als contractuele waarborg voor een in grote lijnen overeenkomstig beschermingsniveau voor naar derde landen doorgegeven gegevens.

De in artikel 46 van de AVG genoemde standaardcontractbepalingen en andere doorgifte-instrumenten opereren niet in een vacuüm. Het Hof stelt dat de als exporteurs optredende verwerkingsverantwoordelijken en verwerkers, per geval en indien van toepassing in samenwerking met de importeur in het derde land, verantwoordelijk zijn voor de controle als de wetgeving of rechtspraktijk in het derde land tekortschiet in de doeltreffendheid van de passende waarborgen voor de in artikel 46 van de AVG genoemde doorgifte-instrumenten. Het Hof laat in die gevallen nog steeds de mogelijkheid open dat de exporteurs aanvullende maatregelen nemen om deze leemten in de bescherming op te vullen en de bescherming op het in de wetgeving van de Unie vereiste niveau te brengen. Het Hof gaat niet nader in op welke maatregelen dat zouden kunnen zijn. Het Hof benadrukt echter wel dat deze door de exporteurs per geval moeten worden vastgesteld. Dit sluit aan bij het beginsel van verantwoordingsplicht in artikel 5, lid 2, van de AVG, waarin verwerkingsverantwoordelijken verantwoordelijk worden gesteld voor de AVG-beginselen met betrekking tot de verwerking van persoonsgegevens en moeten kunnen aantonen dat deze worden nageleefd.

Om exporteurs (ongeacht of dit private of publieke verwerkingsverantwoordelijken of verwerkers zijn die binnen het toepassingsgebied van de AVG persoonsgegevens verwerken) te helpen bij de complexe taak van het beoordelen van derde landen en het waar nodig vaststellen van passende aanvullende maatregelen, heeft het Europees Comité voor gegevensbescherming (EDPB) deze aanbevelingen vastgesteld. Met deze aanbevelingen bieden we exporteurs een reeks te volgen stappen, mogelijke informatiebronnen en enkele voorbeelden van aanvullende maatregelen die kunnen worden getroffen.

Als een **eerste stap** raadt het Comité u, exporteurs, aan **op de hoogte te zijn van wat u doorgeeft**. Het in kaart brengen van alle doorgiften van persoonsgegevens aan derde landen is geen gemakkelijke opgave. Om te waarborgen dat er, ongeacht waar de gegevens verwerkt worden, in grote lijnen een overeenkomstig beschermingsniveau wordt geboden, is het echter noodzakelijk te weten waar de gegevens terechtkomen. Ook moet u controleren of de gegevens die u doorgeeft passend, relevant en tot het noodzakelijke beperkt zijn voor het doel waarmee ze worden doorgegeven aan en verwerkt in een derde land.

Een **tweede** stap is het **controleren van het doorgifte-instrument dat u voor de doorgiften gebruikt** aan de hand van de lijst in hoofdstuk V van de AVG. Indien het land, het gebied of de sector waarnaar de gegevens worden doorgegeven al door de Europese Commissie adequaat is verklaard, middels een van de uit hoofde van artikel 45 van de AVG of de eerdere Richtlijn 95/46 genomen adequaatheidsbesluiten, en mits dit nog geldig is, hoeft u geen verdere stappen te ondernemen dan te bewaken dat het adequaatheidsbesluit nog steeds van kracht is. Bij ontstentenis van een adequaatheidsbesluit moet u voor regelmatige en repetitieve doorgiften gebruikmaken van een van de in artikel 46 van de AVG vermelde doorgifte-instrumenten. Slechts in sommige gevallen van incidentele en niet-repetitieve doorgifte kunt u gebruikmaken van een van de in artikel 49 van de AVG voorziene afwijkingen, indien u aan de voorwaarden voldoet.

Een **derde stap** is het **beoordelen** of er in **het recht of de praktijk van het derde land** iets is wat afbreuk doet aan de doeltreffendheid van de passende waarborgen van de doorgifte-instrumenten die u in het kader van een specifieke doorgifte gebruikt. Bij uw beoordeling moet u zich hoofdzakelijk richten op de relevante wetgeving van het derde land ten aanzien van uw doorgifte en het in artikel 46 van de AVG voorziene doorgifte-instrument waarvan u gebruikmaakt en dat het beschermingsniveau zou kunnen ondermijnen. Voor een evaluatie van de elementen waarmee u rekening moet houden bij de beoordeling van de wetgeving van een derde land inzake toegang tot gegevens door overheidsinstanties voor surveillancedoeleinden, kunt u de aanbevelingen van het EDPB inzake Europese essentiële garanties raadplegen. In het bijzonder moet u deze zorgvuldig in acht nemen als de wetgeving voor de toegang tot gegevens door overheidsinstanties dubbelzinnig of niet openbaar beschikbaar is. Bij ontstentenis van wetgeving met betrekking tot de omstandigheden waaronder overheidsinstanties toegang hebben tot persoonsgegevens moet u, als u met de doorgifte wilt doorgaan, kijken naar andere relevante en objectieve factoren en u niet baseren op subjectieve factoren, zoals hoe groot de kans is dat overheidsinstanties toegang tot de gegevens krijgen op een manier die niet overeenstemt met de Europese normen. Deze beoordeling moet met passende zorgvuldigheid worden uitgevoerd en zorgvuldig worden gedocumenteerd, aangezien u verantwoordelijk wordt gehouden voor het besluit dat u op basis daarvan neemt.

Een **vierde stap** is **het bepalen en vaststellen van de aanvullende maatregelen** die nodig zijn om de doorgegeven gegevens in grote lijnen op het beschermingsniveau te brengen dat voldoet aan de 'overeenkomst in grote lijnen'-norm die geldt in de EU. Deze stap is alleen nodig wanneer uit uw beoordeling blijkt dat de wetgeving van het derde land afbreuk doet aan de doeltreffendheid van het in artikel 46 van de AVG voorziene doorgifte-instrument dat u bij de doorgifte gebruikt of van plan bent te gebruiken. Deze aanbevelingen bevatten (in bijlage 2) een niet-uitputtende lijst met voorbeelden van aanvullende maatregelen en enkele van de voorwaarden waaraan deze moeten voldoen om doeltreffend te zijn. Net als bij de passende waarborgen van de in artikel 46 van de AVG voorziene doorgifte-instrumenten, kunnen sommige aanvullende maatregelen in het ene land wel doeltreffend zijn, en in het andere niet. Het is uw verantwoordelijkheid na te gaan in hoeverre de maatregelen voor uw doorgifte, gelet op de wetgeving van het derde land en het doorgifte-instrument dat u gebruikt, doeltreffend zijn. U wordt verantwoordelijk gehouden voor het besluit dat u op basis daarvan neemt. Wellicht moet u hiervoor ook verschillende aanvullende maatregelen combineren. U kunt uiteindelijk tot de conclusie komen dat u met geen enkele aanvullende maatregel een in grote lijnen overeenkomend beschermingsniveau voor uw specifieke doorgifte kunt bieden. In die gevallen waarin er geen passende aanvullende maatregel voorhanden is, moet u vermijden dat de doorgifte wordt uitgevoerd of deze opschorten of beëindigen, om te voorkomen dat het beschermingsniveau van de persoonsgegevens wordt aangetast. Ook deze beoordeling van aanvullende maatregelen moet met passende zorgvuldigheid worden uitgevoerd en worden gedocumenteerd.

Een **vijfde stap** is het **nemen** van eventuele **formele procedurele stappen** die zijn vereist voor de toepassing van een aanvullende maatregel, afhankelijk van het in artikel 46 van de AVG voorziene instrument voor doorgifte dat u gebruikt. Deze formaliteiten worden in deze aanbevelingen nader omschreven. Voor sommige formaliteiten moet u wellicht de bevoegde toezichthoudende autoriteiten raadplegen.

De **laatste en definitieve stap** is dat u op gezette tijden het beschermingsniveau van de door u aan derde landen doorgegeven gegevens opnieuw beoordeelt en erop toeziet of er ontwikkelingen hebben plaatsgevonden of zullen plaatsvinden die dit kunnen aantasten. Op grond van het beginsel van verantwoordingsplicht is een voortdurende bewaking van het beschermingsniveau van persoonsgegevens vereist.

De toezichthoudende autoriteiten zullen hun mandaat voor toepassing en handhaving van de AVG blijven uitoefenen. De toezichthoudende autoriteiten houden voldoende rekening met de maatregelen die exporteurs nemen om te waarborgen dat het beschermingsniveau van de doorgegeven gegevens in grote lijnen overeenkomt. Zoals het Hof in herinnering brengt, worden doorgiften van gegevens door de toezichthoudende autoriteiten opgeschort of verboden wanneer naar aanleiding van een onderzoek of klacht blijkt dat niet kan worden gewaarborgd dat het beschermingsniveau in grote lijnen overeenstemt.

De toezichthoudende autoriteiten zullen richtsnoeren voor exporteurs blijven ontwikkelen en hun activiteiten binnen het Comité blijven coördineren om een coherente toepassing van de EU-gegevensbeschermingswetgeving te waarborgen.

Inhoudsopgave

Het Europees Comité voor gegevensbescherming

Gezien artikel 70, lid 1, onder e), van Verordening (EU) 2016/679/EU 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"),

Gezien de Overeenkomst betreffende de Europese Economische Ruimte (EER) en met name bijlage XI en Protocol 37 daarbij, zoals gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018[1],

Gezien artikel 12 en artikel 22 van zijn reglement van orde,

Overwegende hetgeen volgt:

(1) Het Hof van Justitie van de Europese Unie (HvJ-EU) concludeert in zijn arrest van 16 juli 2020 in de zaak Data Protection Commissioner tegen Facebook Ireland Ltd, Maximillian Schrems, C-311/18 dat artikel 46, lid 1, en artikel 46, lid 2, onder c), van de AVG aldus moeten worden uitgelegd dat de in deze bepaling vereiste passende waarborgen, afdwingbare rechten en doeltreffende rechtsmiddelen moeten verzekeren dat de rechten van personen wier persoonsgegevens op basis van standaardbepalingen inzake gegevensbescherming naar een derde land worden doorgegeven, in grote lijnen overeenkomen met het beschermingsniveau dat binnen de Europese Unie wordt gewaarborgd door die verordening, gelezen in het licht van het Handvest van de grondrechten van de Europese Unie.[2]

(2) Zoals door het Hof wordt benadrukt, moet een beschermingsniveau van natuurlijke personen dat in grote lijnen overeenkomt met het beschermingsniveau dat binnen de Europese Unie door de AVG wordt gewaarborgd, gelezen in het licht van het Handvest van de grondrechten van de Europese Unie, bijgevolg worden gewaarborgd ongeacht de bepaling van hoofdstuk V op basis waarvan persoonsgegevens naar een derde land worden doorgegeven. De bepalingen van hoofdstuk V van de AVG beogen de continuïteit van het hoge niveau van deze bescherming bij doorgifte van persoonsgegevens naar een derde land te waarborgen.[3]

(3) In overweging 108 en artikel 46, lid 1, van de AVG wordt gesteld dat indien er geen adequaatheidsbesluit is genomen, de verwerkingsverantwoordelijke of de verwerker maatregelen dient te nemen om het ontoereikende niveau van gegevensbescherming in een derde land te verhelpen door middel van passende waarborgen voor de betrokkene. Een verwerkingsverantwoordelijke of verwerker kan passende waarborgen bieden, zonder dat daarvoor specifieke toestemming van een toezichthoudende autoriteit is vereist, door gebruik te maken van een

[1] Alle verwijzingen in dit document naar "lidstaten" moeten worden gelezen als verwijzingen naar "EER-lidstaten".
[2] Arrest van het HvJ-EU van 16 juli 2020 in de zaak Data Protection Commissioner tegen Facebook Ireland Ltd, Maximillian Schrems, (hierna C-311/18 (Schrems II)), tweede vaststelling.
[3] C-311/18 (Schrems II), punten 92 en 93.

van de instrumenten voor doorgiften die worden vermeld in artikel 46, lid 2, van de AVG, zoals standaardbepalingen inzake gegevensbescherming.

(4) Het Hof licht toe dat de door de Commissie vastgestelde standaardbepalingen inzake gegevensbescherming uitsluitend beogen aan de in de Unie gevestigde verwerkingsverantwoordelijken of hun in de Unie gevestigde verwerkers contractuele waarborgen te bieden die in alle derde landen uniform gelden. Gezien het contractuele karakter van de standaardbepalingen inzake gegevensbescherming zijn deze niet bindend voor de overheidsinstanties van derde landen, aangezien zijn geen partij zijn bij het contract. Dientengevolge moeten gegevensexporteurs de in deze standaardbepalingen inzake gegevensbescherming vervatte waarborgen wellicht aanvullen met aanvullende maatregelen om de naleving van het in de EU-wetgeving vereiste beschermingsniveau in een bepaald derde land te verzekeren. Het Hof verwijst naar overweging 109 van de AVG, waarin deze mogelijkheid wordt genoemd en verwerkingsverantwoordelijken en verwerkers worden aangemoedigd hiervan gebruik te maken.[4]

(5) Het Hof stelde dat het bovenal aan die verwerkingsverantwoordelijke of aan zijn verwerker is om van geval tot geval en eventueel in samenwerking met de ontvanger van de doorgifte na te gaan of het recht van het derde land van bestemming vanuit het oogpunt van het Unierecht een passende bescherming waarborgt voor persoonsgegevens die zijn doorgegeven op basis van standaardbepalingen inzake gegevensbescherming, en om zo nodig aanvullende waarborgen te bieden naast de door die bepalingen geboden waarborgen.[5]

(6) Indien de in de Unie gevestigde verwerkingsverantwoordelijke of zijn in de Unie gevestigde verwerker geen toereikende aanvullende maatregelen kunnen nemen om een beschermingsniveau te waarborgen dat in grote lijnen overeenkomt met het niveau krachtens de Unie-wetgeving, zijn zij of, subsidiair, de bevoegde toezichthoudende autoriteit, ertoe verplicht om de doorgifte van persoonsgegevens naar het betrokken derde land op te schorten of te beëindigen.[6]

(7) Noch in de AVG, noch door het Hof wordt gedefinieerd of gepreciseerd waaruit de “extra waarborgen”, “extra maatregelen” of “aanvullende maatregelen” voor de waarborgen voor de in artikel 46, lid 2, van de AVG voorziene doorgifte-instrumenten die de verwerkingsverantwoordelijken en verwerkers nemen om de naleving van het in de Unie-wetgeving vereiste beschermingsniveau voor een bepaald derde land te verzekeren, bestaan.

(8) Het EDPB heeft op eigen initiatief besloten deze vraag te onderzoeken en verwerkingsverantwoordelijken en verwerkers die optreden als exporteurs, aanbevelingen aan te reiken over de te volgen procedure voor het bepalen en vaststellen van aanvullende maatregelen. Deze aanbevelingen zijn bedoeld om de exporteurs een methodologie aan te bieden aan de hand waarvan ze kunnen bepalen of ze extra maatregelen voor hun doorgiften moeten nemen en welke dit zijn. Het is de primaire verantwoordelijkheid van de exporteurs te verzekeren dat het beschermingsniveau van de doorgegeven gegevens in het derde land in grote lijnen overeenkomt met

[4] C-311/18 (Schrems II), punten 132 en 133.
[5] C-311/18 (Schrems II), punt 134.
[6] C-311/18 (Schrems II), punt 135.

het binnen de EU gewaarborgde niveau. Met deze aanbevelingen wil het EDPD, uit hoofde van het mandaat van het EDPD, aanmoedigen dat de AVG en het arrest van het Hof consistent worden toegepast.[7]

HEEFT DE VOLGENDE AANBEVELING VASTGESTELD:

[7] Artikel 70,lid 1, onder e, van de AVG.

1 VERANTWOORDINGSPLICHT BIJ DOORGIFTEN VAN GEGEVENS

1. In de primaire wetgeving van de Unie wordt het recht op gegevensbescherming als een grondrecht beschouwd.[8] Dienovereenkomstig wordt er een hoog beschermingsniveau voor gegevensbescherming geboden en mogen hieraan slechts beperkingen worden gesteld indien hierin is voorzien in het recht, de essentie van het recht wordt geëerbiedigd, de beperkingen evenredig en noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of de vereisten voor de bescherming van de rechten en vrijheden van anderen.[9] Het recht op bescherming van persoonsgegevens heeft geen absolute gelding, maar moet worden beschouwd in relatie tot de functie ervan in de samenleving en moet conform het evenredigheidsbeginsel tegen andere grondrechten worden afgewogen.[10]

2. Om te verzekeren dat het door de AVG gewaarborgde beschermingsniveau niet wordt ondermijnd, moeten de gegevens die worden doorgegeven naar derde landen buiten de EER worden omkleed met een beschermingsniveau dat in grote lijnen overeenkomt met dat binnen de EU.

3. Het recht op gegevensbescherming is actief van aard. Het verplicht exporteurs en importeurs (ongeacht of zij verwerkingsverantwoordelijken en/of verwerkers zijn) verder te gaan dan de erkenning of de passieve naleving van dit recht.[11] Verwerkingsverantwoordelijken en verwerkers moeten actief en doorlopend ernaar streven aan de bescherming van gegevens te voldoen door wettelijke, technische en organisatorische maatregelen te treffen die een doeltreffende bescherming waarborgen. Verwerkingsverantwoordelijken en verwerkers moeten deze inspanningen tevens kunnen aantonen bij het publiek in het algemeen en de autoriteiten die toezicht houden op gegevensbescherming. Dit is het zogenoemde beginsel van verantwoordingsplicht.[12]

4. Het beginsel van verantwoordingsplicht, dat noodzakelijk is om een doeltreffende toepassing van het door de AVG geboden beschermingsniveau te waarborgen, is ook van toepassing op doorgiften van gegevens naar derde landen[13], aangezien deze op zich een vorm van gegevensverwerking zijn.[14] Zoals het Hof in het arrest benadrukt, moet een beschermingsniveau dat in grote lijnen overeenkomt met het beschermingsniveau dat binnen de Europese Unie wordt gewaarborgd door de AVG, gelezen in het licht van het Handvest van de grondrechten van de Europese Uniebeschermingsniveau, bijgevolg worden gewaarborgd ongeacht de bepaling van dat hoofdstuk op basis waarvan persoonsgegevens naar een derde land worden doorgegeven.[15]

5. In de zaak Schrems II benadrukt het Hof de verantwoordelijkheden van exporteurs en importeurs om te verzekeren dat de verwerking van persoonsgegevens is en zal worden uitgevoerd overeenkomstig het in de EU-gegevensbeschermingswetgeving vastgestelde beschermingsniveau en om de doorgifte

[8] Artikel 8, lid 1, van het Handvest van de grondrechten en artikel 16, lid 1, VWEU, preambule 1, artikel 1, lid 2, van de AVG.
[9] Artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie.
[10] Overweging 4 van de AVG en C-507/17 Google LLC, opvolger in rechte van Google Inc. tegen Commission nationale de l'informatique et des libertés (CNIL), punt 60.
[11] C-92/09 en C-93/02, Volker und Markus Schecke GbR tegen Land Hessen, Conclusie van advocaat-generaal Sharpston van 17 juni 2010, punt 71.
[12] Artikel 5, lid 2, en artikel 28, lid 3, onder h), van de AVG.
[13] Artikel 44, en overweging 101 van de AVG en artikel 47, lid 2, onder d), van de AVG.
[14] Arrest van het HvJ-EU van 6 oktober 2015 in de zaak Maximillian Schrems tegen Data Protection Commissioner, (hierna C-362/14 (Schrems I)), punt 45.
[15] C-311/18 (Schrems II), punt 92 en 93.

op te schorten of het contract te beëindigen wanneer de importeur van de gegevens niet of niet meer kan voldoen aan de standaardbepalingen inzake gegevensbescherming die zijn opgenomen in het betreffende contract tussen de exporteur en de importeur.[16] De als exporteur optredende verwerkingsverantwoordelijke of verwerker moet verzekeren dat de importeurs waar nodig met de exporteur bij de uitvoering van deze verantwoordelijkheden samenwerken, bijvoorbeeld door hem op de hoogte te stellen van elke ontwikkeling die van invloed is op het beschermingsniveau van de in het land van de importeur ontvangen persoonsgegevens.[17] Deze verantwoordelijkheden vloeien voort uit de toepassing van het AVG-beginsel van verantwoordingsplicht op het doorgeven van gegevens.[18]

2 ROUTEKAART: TOEPASSING VAN HET BEGINSEL VAN VERANTWOORDINGSPLICHT OP GEGEVENSDOORGIFTEN IN DE PRAKTIJK

6. Hieronder volgt een routekaart van de stappen die u moet nemen om na te gaan of u (de gegevensexporteur) aanvullende maatregelen moet treffen om op legale wijze gegevens buiten de EER door te geven. Onder "U" wordt in dit document verstaan de als exporteur optredende verwerkingsverantwoordelijke of verwerker die binnen het toepassingsgebied van de AVG persoonsgegevens verwerkt, met inbegrip van de verwerking door particuliere instanties en overheidslichamen bij de doorgifte van gegevens aan particuliere lichamen.[19] Met betrekking tot het doorgeven van persoonsgegevens tussen overheidslichamen zijn bijzondere richtsnoeren vastgesteld in het EDPB-document *Richtsnoeren 2/2020 over artikel 46, lid 2, onder a), en artikel 46, lid 3, onder b), van Verordening 2016/679 voor doorgiften van persoonsgegevens tussen overheidsautoriteiten en -lichamen in de EER aan overheden buiten de EER (Engelse tekst).*[20]

7. U dient deze beoordeling en de door u gekozen en getroffen aanvullende maatregelen op gepaste wijze te documenteren. Deze documentatie moet desgevraagd ter beschikking worden gesteld aan de bevoegde toezichthoudende autoriteit.[21]

2.1 Stap 1: Bekendheid met uw doorgiften

8. Om te weten waaraan u (de gegevensexporteur) moet voldoen om de doorgifte van persoonsgegevens voort te zetten of nieuwe doorgiften uit te voeren[22], is de eerste stap ervoor te zorgen dat u volledig op de hoogte bent van wat u doorgeeft (bekendheid met uw doorgiften). Het registreren en in kaart brengen van alle doorgiften kan een lastige opgave zijn voor bedrijven die bij meerdere, uiteenlopende en regelmatige doorgiften met derde landen zijn betrokken en gebruikmaken van een reeks

[16] C-311/18 (Schrems II), punten 134, 135, 139, 140, 141 en 142.
[17] C-311/18 (Schrems II), punt 134.
[18] Artikel 5, lid 2, en artikel 28, lid 3, onder h), van de AVG.
[19] Zie Richtsnoeren 3/2018 van het EDPB over het territoriale toepassingsgebied van de AVG (artikel 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_nl
[20] *Richtsnoeren 2/2020 over artikel 46, lid 2, onder a), en artikel 46, lid 3, onder b), van Verordening 2016/679 voor doorgiften van persoonsgegevens tussen overheidsautoriteiten en -lichamen in de EER aan overheden buiten de EER (Engelse tekst)*; zie https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en
[21] Artikel 5, lid 2, en artikel 24, lid 1), van de AVG.
[22] NB. Onder doorgifte wordt ook verstaan de toegang op afstand van een entiteit in een derde land tot gegevens die zich in de EER bevinden.

verwerkers of subverwerkers. Bekendheid met uw doorgiften is een essentiële eerste stap om te voldoen aan uw verplichtingen uit hoofde van het beginsel van verantwoordingsplicht.

9. Om volledig op de hoogte te zijn van de gegevens die u doorgeeft, kunt u bouwen op het register van verwerkingsactiviteiten dat u mogelijk als verwerkingsverantwoordelijke of verwerker uit hoofde van artikel 30 van de AVG moet bijhouden.[23] Ook eerdere acties om te voldoen aan de verplichting uit hoofde van artikel 13, lid 1, onder f), en artikel 14, lid 1, onder f), van de AVG, om de betrokkenen te informeren over het doorgeven van hun persoonsgegevens aan derde landen, kunnen u daarbij van dienst zijn.[24]

10. Bij het in kaart brengen van de doorgiften moet u niet vergeten ook verdere doorgiften in aanmerking te nemen, bijvoorbeeld of uw verwerkers buiten de EER de door u aan hen toevertrouwde persoonsgegevens doorgeven aan een subverwerker in een ander derde land of hetzelfde derde land[25].

11. In lijn met het AVG-beginsel van "gegevensminimalisatie",[26] moet u controleren of de gegevens die u doorgeeft passend, relevant en tot het noodzakelijke beperkt zijn voor het doel waarmee ze worden doorgegeven aan en verwerkt in een derde land.

12. Deze activiteiten moeten worden uitgevoerd voordat er gegevens worden doorgegeven en moeten na een opschorting van gegevensdoorgiften worden bijgewerkt voordat de doorgiften worden hervat: u moet weten waar de door u geëxporteerde gegevens zich bevinden of door de importeurs worden verwerkt (kaart met bestemmingen).

13. Houd er rekening mee dat toegang op afstand vanuit een derde land (bijvoorbeeld in ondersteuningssituaties) en/of opslag in een cloud buiten de EER, ook als een doorgifte wordt beschouwd.[27] Meer in het bijzonder: als u een internationale cloudinfrastructuur gebruikt, moet u nagaan of uw gegevens worden doorgegeven naar derde landen en welke, tenzij de cloudaanbieder duidelijk in zijn contract aangeeft dat de gegevens helemaal niet in derde landen worden verwerkt.

---

[23] Zie artikel 30 van de AVG en in het bijzonder lid 1, onder e), en lid 2, onder c). Daarnaast moet uw verwerkingsregister een beschrijving van de verwerkingsactiviteiten bevatten (met inbegrip van, maar niet beperkt tot, de categorieën betrokkenen, de categorieën persoonsgegevens en de doeleinden van de verwerking en bepaalde informatie over gegevensdoorgiften). Sommige verwerkingsverantwoordelijken en verwerkers zijn vrijgesteld van de verplichting een verwerkingsregister te houden (artikel 30, lid 5, van de AVG). Zie voor richtsnoeren met betrekking tot deze uitzondering *Article 29 Working Party, Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30.5 GDPR* (bekrachtigd door het Comité op 25 mei 2018).

[24] Uit hoofde van in de AVG vastgestelde regels voor transparantie moet u betrokkenen informeren over doorgiften van persoonsgegevens naar derde landen (artikel 13, lid 1, onder f), en artikel 14, lid 1, onder f), van de AVG). In het bijzonder moet u hen informeren over of er al dan niet een adequaatheidsbesluit van de Commissie bestaat; of, in het geval van doorgiften zoals bedoeld in artikel 46, artikel 47, van de AVG of artikel 49, lid 1, tweede alinea, van de AVG welke de passende of geschikte waarborgen zijn, hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd. De aan de betrokkene verstrekte gegevens moeten correct en actueel zijn, met name in het licht van de rechtspraak van het Hof inzake doorgiften.

[25] Wanneer de verwerkingsverantwoordelijke zijn voorafgaande schriftelijke algemene of specifieke toestemming heeft verleend overeenkomstig het bepaalde in artikel 28, lid 2, van de AVG.

[26] Artikel 5, lid 1, onder c), van de AVG.

[27] Zie vraag 11 van de veelgestelde vragen over het arrest van het Hof van Justitie van de Europese Unie in zaak C-311/18 – Data Protection Commissioner tegen Facebook Ireland Ltd en Maximillian Schrems, EDPB, 23 juli 2020:"er moet rekening mee worden gehouden dat zelfs het verstrekken van toegang tot gegevens vanuit een derde land, bijvoorbeeld voor administratieve doeleinden, ook een doorgifte is".

2.2 Stap 2: Bepaal de doorgifte-instrumenten die u gebruikt

14. Een tweede stap die u moet nemen, is het bepalen van de door u gebruikte doorgifte-instrumenten uit de instrumenten die zijn vermeld en voorzien in hoofdstuk V van de AVG.

Adequaatheidsbesluiten

15. Door middel van **adequaatheidsbesluiten** kan de Europese Commissie voor sommige of alle derde landen waarnaar u persoonsgegevens doorgeeft, erkennen dat zij een passend beschermingsniveau voor persoonsgegevens bieden.[28]

16. Het effect van zo'n adequaatheidsbesluit is dat persoonsgegevens vanuit de EER kunnen worden doorgegeven zonder dat er een in artikel 46 van de AVG voorzien doorgifte-instrument noodzakelijk is.

17. Adequaatheidsbesluiten kunnen betrekking hebben op een heel land of een deel daarvan. Adequaatheidsbesluiten kunnen betrekking hebben op alle doorgiften van gegevens naar een land of op bepaalde soorten doorgiften (b.v. in een bepaalde sector).[29]

18. De adequaatheidsbesluiten worden door de Europese Commissie gepubliceerd op haar website.[30]

19. Als u persoonsgegevens doorgeeft naar derde landen, regio's of sectoren waarover de Commissie een adequaatheidsbesluit heeft genomen (voor zover van toepassing), **hoeft u de volgende stappen in deze aanbevelingen niet uit te voeren.**[31] U moet echter wel blijven controleren of de voor uw doorgiften relevante adequaatheidsbesluiten worden ingetrokken of ongeldig verklaard.[32]

20. Een adequaatheidsbesluit kan echter niet voorkomen dat betrokkenen een klacht indienen. Ook wordt met een adequaatheidsbesluit niet voorkomen dat toezichthoudende autoriteiten een zaak aan een nationale rechtbank voorleggen als zij twijfels hebben over de geldigheid van een besluit, zodat een nationale rechtbank het HvJ-EU kan verzoeken om een prejudiciële verwijzing waarin de geldigheid wordt onderzocht.[33]

---

[28] Op grond van artikel 45 van de AVG heeft de Europese Commissie de bevoegdheid te bepalen of een land buiten de EU een passend beschermingsniveau voor gegevens biedt. Op gelijke wijze heeft de Europese Commissie de bevoegdheid te bepalen of een internationale organisatie een passend beschermingsniveau voor gegevens biedt.

[29] Artikel 45, lid 1, van de AVG.

[30] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[31] Mits u en de gegevensimporteur maatregelen hebben getroffen om te voldoen aan de andere verplichtingen uit hoofde van de AVG; zo niet, moet u die maatregelen nemen.

[32] De Europese Commissie moet periodiek alle adequaatheidsbesluiten opnieuw beoordelen en bewaken of de door de adequaatheidsbesluiten begunstigde derde landen nog steeds een passend beschermingsniveau verzekeren (zie artikel 45, lid 3, en artikel 45, lid 4, van de AVG). Ook kunnen adequaatheidsbesluiten door het HvJ-EU nietig worden verklaard (zie het arrest in de zaak C-362/14 (Schrems I) en de zaak C-311/18 (Schrems II).

[33] C-311/18 (Schrems II), punten 118-120. De toezichthoudende autoriteiten mogen het adequaatheidsbesluit niet naast zich neerleggen en het doorgeven van persoonsgegevens naar dergelijke landen niet opschorten of verbieden door zich uitsluitend te beroepen op het ontoereikende beschermingsniveau. Zij mogen hun bevoegdheid tot het opschorten of verbieden van doorgiften van persoonsgegeven alleen op andere gronden uitoefenen (b.v. schending van artikel 32 van de AVG vanwege onvoldoende beveiligingsmaatregelen of schending van artikel 6 van de AVG als voor de gegevensverwerking als zodanig een geldige rechtsgrondslag ontbreekt). De toezichthoudende autoriteiten mogen, volledig onafhankelijk, onderzoeken of de doorgifte van die gegevens voldoet aan de in de AVG vastgestelde vereisten. Indien van toepassing kunnen ze een procedure

Voorbeeld: De heer Schrems, een EU-burger, diende in juni 2013 een klacht in bij de Irish Data Protection Commission (DPC) en verzocht de toezichthoudende autoriteit om het doorgeven van zijn persoonsgegevens van Facebook Ireland naar de Verenigde Staten te verbieden of op te schorten. Hij was van mening dat het recht en de praktijk in de Verenigde Staten geen passend beschermingsniveau boden voor de in dat gebied bewaarde gegevens tegen de surveillance-activiteiten waar overheidsinstanties van dat land bij betrokken zijn. De DPC wees de klacht af en voerde hiervoor in het bijzonder als grond aan dat de Europese Commissie in Besluit 2000/520 van mening was dat de Verenigde Staten, onder de "veilige haven"-regeling, een passend beschermingsniveau van de doorgegeven gegevens verzekerde (de veiligehavenbeschikking). De heer Schrems ging tegen de beslissing van de DPC in beroep en het Ierse Hooggerechtshof verwees de vraag over de geldigheid van Besluit 2000/520 naar het Hof van Justitie van de Europese Unie (HvJ-EU). Het HvJ-EU besloot vervolgens Besluit 2000/520 van de Commissie inzake de door de veiligehavenbeginselen voor privacy geboden gepastheid van de bescherming, nietig te verklaren.[34]

Artikel 46 van de AVG: doorgifte-instrumenten

21. Artikel 46 van de AVG bevat een reeks doorgifte-instrumenten met "passende waarborgen" die exporteurs kunnen gebruiken voor het doorgeven van persoonsgegevens naar derde landen waarvoor geen adequaatheidsbesluit is vastgesteld. De belangrijkste doorgifte-instrumenten waar artikel 46 van de AVG in voorziet, zijn:

- standaardbepalingen inzake gegevensbescherming;
- bindende bedrijfsvoorschriften;
- gedragscodes;
- certificeringsmechanismen;
- ad-hoc contractuele bepalingen.

22. Ongeacht welk doorgifte-instrument van artikel 46 van de AVG u kiest, moet u ervoor zorgen dat de doorgegeven persoonsgegevens in het algemeen in grote lijnen overeenkomstig worden beschermd.

23. De in artikel 46 van de AVG voorziene doorgifte-instrumenten bevatten hoofdzakelijk passende waarborgen van contractuele aard die toepasbaar zijn op doorgiften naar alle derde landen. De situatie in het derde land waarnaar u de gegevens doorgeeft, kan zodanig zijn dat u deze doorgifte-instrumenten en de daarin vervatte waarborgen moet aanvullen met extra maatregelen ("aanvullende maatregelen") om een in grote lijnen overeenkomend beschermingsniveau te verzekeren.[35]

Afwijkingen

24. Naast de adequaatheidsbesluiten en de in artikel 46 van de AVG voorziene doorgifte-instrumenten, bevat de AVG nog een derde weg om in bepaalde situaties persoonsgegevens door te geven. Indien u voldoet aan bepaalde voorwaarden kunt u nog steeds persoonsgegevens doorgeven op grond van een van de in artikel 49 van de AVG vermelde afwijkingen.

aanspannen bij de nationale rechtbanken zodat deze, bij twijfels over de geldigheid van het adequaatheidsbesluit van de Commissie, het HvJ-EU om een prejudiciële verwijzing kunnen verzoeken waarin de geldigheid wordt onderzocht.

[34] Zaak C-362/14 (Schrems I).

[35] C-311/18 (Schrems II), punten 130 en 133. Zie hieronder ook punt 2, lid 3.

25. Artikel 49 van de AVG is uitzonderlijk van aard. De daarin opgenomen afwijkingen moeten restrictief worden uitgelegd en hoofdzakelijk betrekking hebben op incidentele en niet-repetitieve verwerkingsactiviteiten. Het EDPB heeft hiervoor de Richtsnoeren 2/2018 inzake afwijkingen op grond van artikel 49 van Verordening 2016/679 uitgebracht. [36]

26. Voordat u gebruikmaakt van een afwijking op grond van artikel 49 van de AVG, moet u controleren of uw doorgifte voldoet aan de strikte criteria die in deze bepaling voor elke afwijking zijn vastgesteld.

***

27. Als er voor uw doorgifte geen rechtsgrondslag bestaat in een adequaatheidsbesluit, noch in een afwijking van artikel 49, moet u doorgaan met stap 3.

2.3 Stap 3: Beoordeel of het door u gebruikte doorgifte-instrument van artikel 46 van de AVG doeltreffend is in het licht van alle omstandigheden van de doorgifte.

28. Het kiezen van een in artikel 46 van de AVG voorzien doorgifte-instrument is mogelijk niet genoeg. Het doorgifte-instrument moet de zekerheid bieden dat het door de AVG gewaarborgde beschermingsniveau niet door de doorgifte wordt ondermijnd.[37] Met andere woorden: uw doorgifte-instrument moet in de praktijk doeltreffend zijn.

29. Doeltreffend houdt in dat de doorgegeven persoonsgegevens in het derde land een beschermingsniveau genieten dat in grote lijnen overeenkomt met het in de EER gewaarborgde niveau.[38] Dit is niet het geval als de gegevensimporteur niet kan voldoen aan de verplichtingen voor het gekozen in artikel 46 van de AVG voorziene doorgifte-instrument, op grond van de wetgeving en praktijken die in het derde land op de doorgifte van toepassing zijn.

30. U moet derhalve, in voorkomend geval samen met de importeur, nagaan of er in de wetgeving of praktijk van het derde land iets is wat afbreuk doet aan de doeltreffendheid van de passende waarborgen van de in artikel 46 van de AVG voorziene doorgifte-instrumenten die u in het kader van een specifieke doorgifte gebruikt. In voorkomend geval moet uw gegevensimporteur u de relevante bronnen en informatie over het derde land waarin hij is gevestigd, verstrekken en de voor de doorgifte toepasselijke wetgeving. U kunt ook andere informatiebronnen raadplegen, bijvoorbeeld in de niet-uitputtende lijst in bijlage 3.[39]

31. Bij uw beoordeling moet u rekening houden met alle bij de doorgifte betrokken actoren die u bij het in kaart brengen van doorgiften hebt geïdentificeerd (b.v. verwerkingsverantwoordelijken, verwerkers en subverwerkers die gegevens in het derde land verwerken). Hoe meer verwerkingsverantwoordelijken, verwerkers en importeurs er betrokken zijn, hoe ingewikkelder uw beoordeling zal zijn. Bij deze beoordeling moet u ook rekening houden met een mogelijke verdere doorgifte van de gegevens.

32. Hiervoor moet u de kenmerken van alle doorgiften afzonderlijk onderzoeken en bepalen hoe de nationale rechtsorde van het land waarnaar de gegevens worden doorgegeven (of verder worden doorgegeven), op deze doorgiften van toepassing is.

---

[36] Meer informatie hierover vindt u op https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-22018-derogations-article-49-under-regulation_nl.
[37] Artikel 44 van de AVG.
[38] C-311/18 (Schrems II), punt 105 en tweede vaststelling.
[39] Zie ook punt 43 hieronder.

33. Welk rechtskader van toepassing is, is afhankelijk van de omstandigheden bij de doorgifte, in het bijzonder:

- het doel waarvoor de gegevens worden doorgegeven en verwerkt (b.v. marketing, personeelszaken, opslag, IT-ondersteuning, medische testen);
- de soorten entiteiten die bij de verwerking zijn betrokken (overheid/particulier, verwerkingsverantwoordelijke/verwerker);
- de sector waarin de doorgifte plaatsvindt (b.v. reclametechnologie, telecommunicatie, financieel, enz.);
- de categorieën van doorgegeven persoonsgegevens (persoonsgegevens die op kinderen betrekking hebben, kunnen bijvoorbeeld onder het toepassingsgebied van specifieke wetgeving in het derde land vallen);
- of de gegevens in het derde land worden bewaard of dat er alleen toegang op afstand is tot gegevens die in de EU/EER worden bewaard;
- de indeling van de gegevens die worden doorgegeven (d.w.z. in platte tekst, gepseudonimiseerd of versleuteld[40]);
- de mogelijkheid dat de gegevens verder worden doorgegeven van het derde land naar een ander derde land.[41]

34. Ten aanzien van de toepasselijke wetgeving moet u beoordelen of er bepalingen zijn die afbreuk doen aan de verplichtingen voor het in artikel 46 van de AVG voorziene doorgifte-instrument dat u hebt gekozen. U moet controleren of de verplichtingen op grond waarvan betrokkenen hun rechten in het kader van internationale doorgiften kunnen uitoefenen (zoals verzoeken tot toegang, correctie en verwijdering van doorgegeven gegevens), in de praktijk op doeltreffende wijze kunnen worden toegepast en niet worden gehinderd door de wetgeving in het derde land van bestemming.

35. U moet de betrokken regelgeving van algemene aard beoordelen voor zover deze van invloed is op de doeltreffende toepassing van de waarborgen voor de in artikel 46 van de AVG voorziene doorgifte-instrumenten en de grondrechten van burgers (in het bijzonder het aan de betrokkene verleende recht op verhaal in het geval van toegang tot de doorgegeven gegevens door overheidsinstanties van een derde land).

36. U moet in ieder geval bijzondere aandacht besteden aan mogelijke relevante wetgeving, met name wetgeving waarin voorschriften voor het vrijgeven van persoonsgegevens aan overheidsinstanties zijn neergelegd of waarin aan dergelijke overheidsinstanties bevoegdheden tot toegang tot persoonsgegevens worden verleend (bijvoorbeeld met het oog op handhaving van het strafrecht, toezicht op de regelgeving en nationale veiligheidsoverwegingen. Indien deze voorschriften of bevoegdheden zijn beperkt tot hetgeen in een democratische samenleving noodzakelijk en evenredig is,[42] doen zij geen afbreuk aan het in artikel 46 van de AVG voorziene doorgifte-instrument dat u gebruikt.

---

[40] In sommige landen is het niet toegestaan versleutelde gegevens te importeren.

[41] Wanneer de verwerkingsverantwoordelijke zijn voorafgaande schriftelijke algemene of specifieke toestemming heeft verleend overeenkomstig het bepaalde in artikel 28, lid 2, van de AVG.

[42] Zie artikelen 47 en 52 van het Handvest van de grondrechten van de EU, artikel 23, lid 1, van de AVG en Aanbevelingen 02/2020 van het EDPB inzake Europese essentiële garanties voor surveillancemaatregelen, 10 november 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

37. Als referentie moet u de Europese normen, zoals artikelen 47 en 52 van het Handvest van de grondrechten van de EU, gebruiken om na te gaan of een dergelijke toegang door overheidsinstanties is beperkt tot wat in een democratische samenleving noodzakelijk en evenredig is en of de betrokkenen doeltreffende verhaalmogelijkheden wordt toegekend.

38. Bij het uitvoeren van deze beoordeling zijn ook de verschillende aspecten van het rechtssysteem van dat derde land, b.v. de in artikel 45, lid 2, van de AVG genoemde elementen, van belang.[43] Zo kan de rechtspraktijk in een derde land van belang zijn om te beoordelen in hoeverre de voor personen beschikbare mechanismen voor het instellen van beroep (in rechte) tegen onrechtmatige overheidstoegang tot persoonsgegevens, doeltreffend zijn. Het bestaan van een uitgebreide wet inzake gegevensbescherming of een onafhankelijke gegevensbeschermingsautoriteit, evenals het naleven van internationale instrumenten voor gegevensbeschermingswaarborgen, kan ertoe bijdragen dat de evenredigheid van de overheidsinterventie is verzekerd.[44]

***

39. In de aanbevelingen van het EDPB inzake Europese essentiële garanties wordt aangegeven welke elementen moeten worden beoordeeld om vast te stellen of het rechtskader waarin de toegang tot persoonsgegevens door overheidsinstanties (op het gebied van nationale veiligheid of rechtshandhaving) in een derde land is geregeld, als een te rechtvaardigen aantasting kan worden beschouwd (en dus geen afbreuk doet aan de verplichtingen voor het in artikel 46 van de AVG voorziene doorgifte-instrument) of niet. In het bijzonder moet u deze zorgvuldig in acht nemen als de wetgeving voor de toegang tot gegevens door overheidsinstanties dubbelzinnig of niet openbaar beschikbaar is.

40. Door de aanbevelingen van het EDPB inzake Europese essentiële garanties toe te passen op de situatie van gegevensdoorgiften op basis van de in artikel 46 voorziene doorgifte-instrumenten, beschikken de gegevensexporteur en de gegevensimporteur over richtsnoeren om te beoordelen of dergelijke bevoegdheden een niet te rechtvaardigen aantasting vormen van de verplichtingen van de gegevensimporteur om een in grote lijnen overeenkomend beschermingsniveau te bieden.

41. Het ontbreken van een in grote lijnen overeenkomend beschermingsniveau is met name duidelijk wanneer de wetgeving of rechtspraktijk van het bij uw doorgifte betrokken land niet voldoet aan de voorschriften in de Europese essentiële garanties.

42. Uw beoordeling moet in eerste instantie en met name zijn gebaseerd op de wetgeving die publiekelijk beschikbaar is. In sommige situaties is dit echter niet voldoende, omdat er in de derde landen niet in deze wetgeving is voorzien. In dat geval moet u, als u nog steeds overweegt de doorgifte uit te voeren, kijken naar andere relevante en objectieve factoren[45] en u niet baseren op subjectieve factoren, zoals hoe groot de kans is dat overheidsinstanties toegang tot de gegevens krijgen op een manier die niet overeenkomt met de Europese normen. Deze beoordeling moet met passende zorgvuldigheid worden

[43] C-311/18 (Schrems II), punt 104.
[44] Een voorbeeld: Verdrag 108 (Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, ETS nr. 108) of Verdrag 108+ (gemoderniseerd Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, CETS nr. 223) bieden afdwingbare, internationale rechtsmiddelen voor schendingen van gegevensbescherming en dragen bij tot het bieden van een minimaal beschermingsniveau voor persoonsgegevens en eerbiediging van het privéleven.
[45] Zie punt 43 hieronder en bijlage 3.

uitgevoerd en zorgvuldig worden gedocumenteerd, aangezien u verantwoordelijk wordt gehouden voor het besluit dat u op basis daarvan neemt.[46]

43. U kunt uw beoordeling voltooien met informatie uit andere bronnen[47], zoals:

- elementen waaruit blijkt dat de instantie van een derde land, gelet op de gemelde precedenten, wetgeving en praktijken, zal proberen met of zonder medeweten van de gegevensimporteur toegang tot de gegevens te krijgen;
- elementen waaruit blijkt dat de instantie van een derde land, gelet op de gemelde precedenten, wettelijke bevoegdheden en tot haar beschikking staande middelen op technisch, financieel en personeelsgebied, in staat is via de gegevensimporteur of via interceptie van het communicatiekanaal zich toegang tot de gegevens te verschaffen.

44. Uit uw beoordeling kan uiteindelijk blijken dat het door u gebruikte doorgifte-instrument van artikel 46 van de AVG en de daarin vervatte passende waarborgen:

- op doeltreffende wijze ervoor zorgen dat de doorgegeven persoonsgegevens in het derde land een beschermingsniveau genieten dat in grote lijnen overeenkomt met het in de EER gewaarborgde niveau. de gegevensimporteur op grond van de voor de doorgifte geldende wetgeving en praktijken van het derde land in staat stellen aan zijn uit hoofde van het gekozen doorgifte-instrument aangegane verplichtingen te voldoen. U moet dit op gezette tijden, of wanneer er belangrijke wijzigingen aan het licht komen, opnieuw beoordelen (zie stap 6);
- niet op doeltreffende wijze een in grote lijnen overeenkomend beschermingsniveau bieden. Vanwege de voor de doorgifte geldende wetgeving en/of praktijken in het derde land kan de gegevensimporteur niet aan zijn verplichtingen voldoen. Het HvJ-EU heeft benadrukt dat wanneer de in artikel 46 van de AVG voorziene doorgifte-instrumenten tekortschieten, de gegevensexporteur de verantwoordelijkheid heeft om ofwel doeltreffende aanvullende maatregelen te treffen of de persoonsgegevens niet door te geven.[48]

[46] Art. 5, lid 2, van de AVG.
[47] Zie ook bijlage 3.
[48] HvJ-EU C-311/18 (Schrems II), punten 134-135.

Zo was het HvJ-EU van mening dat in Section 702 van de [Foreign Intelligence Surveillance Act (FISA) (wet betreffende het toezicht op buitenlandse inlichtingen)] niet de uit het beginsel van evenredigheid voortvloeiende minimale waarborgen krachtens EU-recht worden geëerbiedigd en dat deze niet kunnen worden beschouwd als beperkt tot wat strikt noodzakelijk is. Dit betekent dat het beschermingsniveau van de onder Section 702 van de FISA goedgekeurde programma's niet in grote lijnen overeenkomt met de krachtens EU-recht verplichte waarborgen. Dit heeft tot gevolg dat onder Section 702 van de FISA[49] vallende gegevensimporteurs of verdere ontvangers aan wie de gegevensimporteur de gegevens vrijgeeft, voor een dergelijke doorgifte uitsluitend standaardcontractbepalingen of andere in artikel 46 van de AVG voorziene doorgifte-instrumenten mogen gebruiken als de toegang tot de doorgegeven gegevens middels extra aanvullende maatregelen onmogelijk of ineffectief wordt gemaakt.

2.4 Stap 4: Aanvullende maatregelen aannemen

45. Als uit de beoordeling van stap 3 is gebleken dat uw in artikel 46 van de AVG voorziene doorgifte-instrument niet doeltreffend is, moet u, in voorkomend geval samen met de importeur, overwegen of er aanvullende maatregelen bestaan die, in aanvulling op de in de doorgifte-instrumenten vervatte waarborgen, verzekeren dat de doorgegeven gegevens in het derde land een beschermingsniveau genieten dat in grote lijnen overeenkomt met het binnen de Unie gewaarborgde beschermingsniveau.[50] Per definitie zijn "aanvullende maatregelen" aanvullend op de reeds voor het doorgifte-instrument van artikel 46 van de AVG bepaalde waarborgen.[51]

46. Wanneer u een bepaald in artikel 46 van de AVG voorzien doorgifte-instrument gebruikt, moet u van geval tot geval vaststellen welke aanvullende maatregelen voor een reeks doorgiften naar een specifiek derde land doeltreffend kunnen zijn. U kunt hierbij voortbouwen op de beoordelingen die u eerder in de stappen (1, 2 en 3 hierboven) hebt uitgevoerd en de potentiële doeltreffendheid van de aanvullende maatregelen voor het verzekeren van het vereiste beschermingsniveau afzetten tegen de uitkomsten daarvan.

47. In beginsel kunnen aanvullende maatregelen contractueel, technisch of organisatorisch van aard zijn. Door verschillende maatregelen te combineren op een wijze dat zij elkaar ondersteunen en op elkaar aansluiten, kan een hoger beschermingsniveau worden bereikt en derhalve worden bijgedragen aan het bereiken van de EU-normen.

48. In het algemeen zal de toegang tot persoonsgegevens door overheidsinstanties van het derde land (waar dit op niet te rechtvaardigen wijze de verplichtingen van de gegevensimporteur om een in grote lijnen overeenkomend beschermingsniveau te bieden, aantast) niet worden ondervangen met

[49] FISA 702 is van toepassing wanneer de gegevens zijn verkregen "uit of met behulp van een aanbieder van elektronische communicatiediensten" (Section 702 FISA = 50 USC § 1881a, onder (h)(2)(A)(vi)), die op zijn beurt in 50 USC § 1881(b)(4) is gedefinieerd als
"(A) een drager van telecommunicatie, volgens de definitie van die term in section 153 van title 47;
(B) een aanbieder van een elektronische communicatiedienst, volgens de definitie van die term in section 2510 van title 18;
(C) een aanbieder van computerdiensten op afstand, volgens de definitie van die term in section 2711 van title 18;
(D) elke andere aanbieder van communicatiediensten die toegang heeft tot bekabelde of elektronische communicatie hetzij tijdens de verzending van die communicatie of tijdens de opslag; of
(E) een medewerker, werknemer of vertegenwoordiger van een onder (A), (B), (C) of (D) beschreven entiteit."
[50] C-311/18 (Schrems II), punt 96.
[51] Overweging 109 van de AVG en C-311/18 (Schrems II), punt 133.

uitsluitend contractuele en organisatorische maatregelen. Er zullen inderdaad situaties zijn waarin uitsluitend technische maatregelen de toegang tot persoonsgegevens door overheidsinstanties in derde landen, met name voor surveillancedoeleinden, kunnen verhinderen of buiten werking kunnen stellen.[52] In dergelijke situaties kunnen contractuele of organisatorische maatregelen een aanvulling vormen op technische maatregelen en het algemene beschermingsniveau van de gegevens versterken, bijvoorbeeld door hindernissen op te werpen voor pogingen van overheidsinstanties om toegang te krijgen tot gegevens op een wijze die niet voldoet aan de normen in de EU.

49. Om te bepalen welke aanvullende maatregelen het meest doeltreffend zijn voor de bescherming van de doorgegeven gegevens kunt u, in voorkomend geval samen met de gegevensimporteur, kijken naar de onderstaande (niet-uitputtende) lijst met elementen:

- de indeling van de gegevens die worden doorgegeven (d.w.z. in platte tekst, gepseudonimiseerd of versleuteld);
- de aard van de gegevens;
- de lengte en complexiteit van de werkstroom voor gegevensverwerking, het aantal bij de verwerking betrokken actoren en hun onderlinge relaties (zijn er bijvoorbeeld meerdere verwerkingsverantwoordelijken of zowel verwerkingsverantwoordelijken als verwerkers betrokken, of zijn er verwerkers betrokken die de gegevens van u doorgeven aan uw gegevensimporteur (gelet op de relevante bepalingen die voor hen gelden uit hoofde van de wetgeving van het derde land van bestemming));[53]
- de mogelijkheid dat de gegevens verder worden doorgegeven, binnen hetzelfde derde land of zelfs naar derde landen (b.v. als er subverwerkers van de gegevensimporteur betrokken zijn[54]).

Voorbeelden van aanvullende maatregelen

50. Enkele voorbeelden van technische, contractuele en organisatorische maatregelen die in overweging kunnen worden genomen, zijn te vinden in de niet-uitputtende lijst in bijlage 2.

***

51. Als u doeltreffende aanvullende maatregelen hebt genomen waarmee u, in combinatie met het door u gekozen doorgifte-instrument van artikel 46 van de AVG, een beschermingsniveau bereikt dat nu in grote lijnen overeenkomt met het in de EER gewaarborgde beschermingsniveau, kunt u uw doorgiften door laten gaan.

[52] Waar dergelijke toegang verder gaat dan in een democratische samenleving noodzakelijk en evenredig is; zie artikelen 47 en 52 van het Handvest van de grondrechten van de EU, artikel 23, lid 1, van de AVG en Aanbevelingen 02/2020 van het EDPB inzake Europese essentiële waarborgen voor surveillancemaatregelen, 10 november 2020 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[53] In de AVG worden aan verwerkingsverantwoordelijken en verwerkers uiteenlopende verplichtingen opgelegd. Doorgiften kunnen plaatsvinden van verwerkingsverantwoordelijke naar verwerkingsverantwoordelijke, tussen samenwerkende verwerkingsverantwoordelijken, van verwerkingsverantwoordelijke naar verwerker en, behoudens goedkeuring van de verwerkingsverantwoordelijke, van verwerker naar verwerkingsverantwoordelijke of van verwerker naar verwerker.

[54] Zie voetnoot 25.

52. Wanneer u geen doeltreffende aanvullende maatregelen kunt vinden of uitvoeren om te waarborgen dat de doorgegeven gegevens in grote lijnen een overeenkomend beschermingsniveau genieten,[55] moet u niet beginnen met het doorgeven van persoonsgegevens naar het betreffende derde land op basis van het in artikel 46 van de AVG voorziene doorgifte-instrument dat u gebruikt. Als u reeds gegevens doorgeeft, bent u verplicht de doorgifte van persoonsgegevens op te schorten of te beëindigen.[56] Uit hoofde van de waarborgen die zijn vervat in het in artikel 46 van de AVG voorziene doorgifte-instrument dat u gebruikt, moeten de gegevens die al naar dat derde land zijn doorgegeven en de kopieën daarvan aan u worden teruggezonden of in zijn geheel door de importeur worden vernietigd.[57]

Voorbeeld: het recht van het derde land verbiedt de aanvullende maatregelen die u hebt bepaald (bijvoorbeeld een verbod op het gebruik van versleuteling) of verhindert anderszins de doeltreffendheid ervan. U mag niet beginnen met het doorgeven van persoonsgegevens naar dit land of u moet lopende bestaande doorgiften naar dit land stopzetten.

53. Als u besluit de doorgifte voort te zetten ondanks het feit dat de importeur de op grond van het in artikel 46 van de AVG voorziene doorgifte-instrument op zich genomen verplichtingen niet kan naleven, moet u de bevoegde toezichthoudende autoriteit hiervan in kennis stellen overeenkomstig de nadere bepalingen die hiervoor in het betrokken in artikel 46 van de AVG voorziene doorgifte-instrument zijn ingevoegd.[58] De doorgiften van gegevens worden door de bevoegde toezichthoudende autoriteit opgeschort of verboden wanneer deze van mening is dat er geen waarborg is dat het beschermingsniveau in grote lijnen overeenstemt.[59]

54. Indien u de doorgifte start of voortzet ondanks het feit dat u niet kunt aantonen dat in het derde land een in grote lijnen overeenkomend beschermingsniveau wordt geboden, kan de bevoegde toezichthoudende autoriteit een corrigerende maatregel opleggen (b.v. een boete).

2.5 Stap 5: Procedurele stappen na het bepalen van doeltreffende aanvullende maatregelen

55. Afhankelijk van het in artikel 46 van de AVG voorziene doorgifte-instrument dat u gebruikt of van plan bent te gebruiken, verschillen de procedurele stappen die u moet nemen als u de te treffen doeltreffende aanvullende maatregelen hebt bepaald.

[55] Waar dergelijke toegang verder gaat dan in een democratische samenleving noodzakelijk en evenredig is; zie artikelen 47 en 52 van het Handvest van de grondrechten van de EU, artikel 23, lid 1, van de AVG en Aanbevelingen 02/2020 van het EDPB inzake Europese essentiële waarborgen voor surveillancemaatregelen, 10 november 2020 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[56] C-311/18 (Schrems II), punt 135.

[57] Zie clausule 12 in de bijlage bij Besluit 87/2010 inzake modelcontractbepalingen; zie de (optionele) extra beëindigingsclausule in bijlage B van 2004/915/EG inzake modelcontractbepalingen.

[58] Zie het EDPB-document Veelgestelde vragen over het arrest van het Hof van Justitie van de Europese Unie in zaak C-311/18 – Data Protection Commissioner tegen Facebook Ireland Ltd en Maximillian Schrems zoals vastgesteld op 23 juli 2020 en met name vraag 5, 6 en 9. Zie ook clausule 4, onder g), van Besluit 2010/87/EU van de Commissie, clausule 5, onder a), van Beschikking 2001/497/EG van de Commissie en "Reeks II", clausule II, onder c), van de bijlage bij Beschikking 2004/915/EG van de Commissie.

[59] C-311/18 (Schrems II), punten 113 en 121.

2.5.1 Standaardbepalingen inzake gegevensbescherming (hierna "standaardcontractbepalingen" genoemd) (artikel 46, lid 2, onder c), en d), van de AVG)

56. Wanneer u in aanvulling op de standaardcontractbepalingen ook voornemens bent aanvullende maatregelen te treffen, hoeft u voor dit soort bepalingen of extra waarborgen niet de bevoegde toezichthoudende autoriteit om goedkeuring te verzoeken, mits de bepaalde aanvullende maatregelen niet direct of indirect in tegenspraak zijn met de standaardcontractbepalingen en in voldoende mate verzekeren dat het door de AVG gewaarborgde beschermingsniveau niet wordt ondermijnd.[60] De gegevensexporteur en de importeur moeten ervoor zorgen dat aanvullende bepalingen niet zodanig kunnen worden uitgelegd dat de rechten en verplichtingen in de standaardcontractbepalingen worden beperkt of er anderszins een lager beschermingsniveau wordt geboden. Overeenkomstig het beginsel van verantwoordingsplicht en uw verplichting om een voldoende gegevensbeschermingsniveau te verstrekken, moet u dit kunnen aantonen, waarbij geen van de bepalingen voor dubbelzinnige uitleg vatbaar mag zijn. De bevoegde toezichthoudende autoriteiten beschikken over de bevoegdheid om deze aanvullende bepalingen waar nodig te beoordelen (b.v. in geval van een klacht of onderzoek op eigen initiatief).

57. Wanneer u voornemens bent de standaardbepalingen inzake gegevensbescherming zelf te wijzigen of wanneer de toegevoegde aanvullende maatregelen direct of indirect "in tegenspraak" zijn met de standaardcontractbepalingen, wordt u geacht u niet langer op standaardcontractbepalingen[61] te baseren en moet u de bevoegde toezichthoudende autoriteit om goedkeuring verzoeken overeenkomstig artikel 46, lid 3, onder a), van de AVG.

2.5.2 Bindende bedrijfsvoorschriften (artikel 46, lid 2, onder b), van de AVG)

58. De in het arrest in de zaak Schrems II gevolgde redenering is ook van toepassing op andere doorgifte-instrumenten overeenkomstig artikel 46, lid 2, van de AVG. Al deze instrumenten hebben immers in principe een contractueel karakter, waardoor overheidsinstanties in derde landen niet zijn gebonden aan de voorziene waarborgen en de door de partijen aanvaarde verplichtingen.[62]

---

[60] Overweging 109 van de AVG: "Dat de verwerkingsverantwoordelijke of de verwerker gebruik kan maken van standaardbepalingen inzake gegevensbescherming die zijn vastgesteld door de Commissie of een toezichthoudende autoriteit, dient niet in te houden dat hij de standaardbepalingen inzake gegevensbescherming niet in een bredere overeenkomst mag opnemen, zoals een overeenkomst tussen de verwerker en een andere verwerker, of geen andere bepalingen of extra waarborgen mag toevoegen, mits deze niet direct of indirect in tegenspraak zijn met de door de Commissie of een toezichthoudende autoriteit vastgestelde standaardcontractbepalingen en geen afbreuk doen aan de grondrechten of de fundamentele vrijheden van de betrokkenen." De door de Europese Commissie uit hoofde van Richtlijn 95/45/EG goedgekeurde reeksen standaardcontractbepalingen voorzien in soortgelijke bepalingen.

[61] Zie analoog hieraan het reeds door het Comité vastgestelde Advies 17/2020 over het door de Sloveense toezichthoudende autoriteit voorgelegde ontwerp voor standaardcontractbepalingen (artikel 28, lid 8 van de AVG) inzake artikel 28, dat een vergelijkbare bepaling bevat ("Daarnaast brengt het Comité in herinnering dat de mogelijkheid van het gebruik van de door een toezichthouder goedgekeurde standaardcontractbepalingen de partijen er niet van weerhoudt overige artikelen of aanvullende waarborgen op te nemen, op voorwaarde dat deze niet direct of indirect strijdig zijn met de goedgekeurde standaardcontractbepalingen of afdoen aan de fundamentele rechten of vrijheden van de betrokkenen. Indien de standaardbepalingen inzake gegevensbescherming worden gewijzigd, worden de partijen bovendien niet langer geacht de goedgekeurde standaardcontractbepalingen te hebben uitgevoerd"), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_nl.pdf.

[62] HvJ-EU, C-311/18 (Schrems II), punt 132.

59. Het arrest in de zaak Schrems II is van belang voor doorgiften van persoonsgegevens op basis van bindende bedrijfsvoorschriften, aangezien het recht in derde landen de door dergelijke instrumenten geboden bescherming kunnen aantasten. Er is nog een discussie gaande over de precieze gevolgen van het Schrems II-arrest voor bindende bedrijfsvoorschriften. Het EDPB zal zo spoedig mogelijk meer informatie verschaffen over de vraag of er in de bindende bedrijfsvoorschriften aanvullende verplichtingen moeten worden opgenomen in de verwijzingsdocumenten WP256/257.[63]

60. Het Hof benadrukte dat het de verantwoordelijkheid van de gegevensexporteur en de gegevensimporteur is om na te gaan of het door het Unierecht vereiste beschermingsniveau in het desbetreffende derde land in acht wordt genomen om te kunnen bepalen of de waarborgen van de standaardcontractbepalingen of de bindende bedrijfsvoorschriften in de praktijk kunnen worden nageleefd. Indien dit niet het geval is, moet u nagaan of u aanvullende maatregelen kunt nemen om een beschermingsniveau te bieden dat in grote lijnen overeenkomt met dat van de EER, en of het recht of de praktijk van het derde land geen afbreuk zal doen aan deze aanvullende maatregelen om de doeltreffendheid ervan in de weg te staan.

2.5.3 Ad-hoc contractuele bepalingen (artikel 46, lid 3, onder a), van de AVG)

61. De in het arrest in de zaak Schrems II gevolgde redenering is ook van toepassing op andere doorgifte-instrumenten overeenkomstig artikel 46, lid 2, van de AVG. Al deze instrumenten hebben immers in de grond een contractueel karakter, waardoor overheidsinstanties in derde landen niet zijn gebonden aan de voorziene waarborgen en de door de partijen aanvaarde verplichtingen.[64] Het arrest in de zaak Schrems II is derhalve van belang voor doorgiften van persoonsgegevens op basis van ad-hoc contractuele bepalingen, aangezien het recht in derde landen de door dergelijke instrumenten geboden bescherming kunnen aantasten. Er is nog discussie over de precieze gevolgen van het Schrems II-arrest voor ad-hoc contractuele bepalingen. Het Comité zal zo spoedig mogelijk meer informatie verschaffen.

2.6 Stap 6: Op gezette tijden opnieuw evalueren

62. U moet doorlopend en in voorkomend geval samen met gegevensimporteurs bewaken of er in het derde land waarnaar u persoonsgegevens hebt doorgegeven, ontwikkelingen hebben plaatsgevonden die van invloed zijn op uw aanvankelijke beoordeling van het beschermingsniveau en de beslissingen die u dienovereenkomstig ten aanzien van uw doorgiften hebt genomen. De verantwoordingsplicht is een aanhoudende verplichting (artikel 5, lid 2, van de AVG).

63. U moet goede mechanismen instellen die in voldoende mate verzekeren dat u doorgiften meteen opschort of beëindigt wanneer:

- de importeur inbreuk heeft gepleegd op of niet kan voldoen aan de verplichtingen op grond van het in artikel 46 van de AVG voorziene doorgifte-instrument; of
- de aanvullende maatregelen in dat derde land niet langer doeltreffend zijn.

[63] Groep gegevensbescherming artikel 29, werkdocument waarin een tabel wordt opgezet met de elementen en beginselen die de bindende bedrijfsvoorschriften moeten bevatten, zoals voor het laatst herzien en goedgekeurd op 6 februari 2018, WP 256 rev.01; Groep gegevensbescherming artikel 29, werkdocument waarin een tabel wordt opgezet met de elementen en beginselen die de bindende bedrijfsvoorschriften moeten bevatten, zoals voor het laatst herzien en goedgekeurd op 6 februari 2018, WP 257 rev.01;
[64] HvJ-EU, C-311/18 (Schrems II), punt 132.

3 CONCLUSIE

64. In de AVG zijn regels neergelegd inzake de verwerking van persoonsgegevens in de EER, waardoor een vrij verkeer van persoonsgegevens binnen de EER mogelijk wordt gemaakt. In hoofdstuk V van de AVG zijn de doorgiften van persoonsgegevens aan derde landen geregeld en worden daaraan hoge eisen gesteld: de doorgifte mag het in de AVG gewaarborgde beschermingsniveau van natuurlijke personen niet ondermijnen (artikel 44 van de AVG). In het arrest in de zaak C-311/18 (Schrems II) benadrukt het HvJ-EU de noodzaak de continuïteit van het in de AVG verleende beschermingsniveau bij doorgifte van persoonsgegevens naar een derde land te waarborgen.[65]

65. Om te waarborgen dat het beschermingsniveau van uw gegevens in grote lijnen daarmee overeenkomt, moet u in de eerste plaats en met name goed op de hoogte zijn van uw doorgiften. Ook moet u nagaan of de gegevens die u doorgeeft passend, relevant en tot het noodzakelijke beperkt zijn voor het doel waarmee ze worden doorgegeven aan en verwerkt in een derde land.

66. Ook moet u bepalen welk doorgifte-instrument u voor uw doorgiften gebruikt. Indien het doorgifte-instrument niet een adequaatheidsbesluit is, moet u van geval tot geval nagaan of het recht of de rechtspraktijk van het derde land van bestemming de waarborgen van de in artikel 46 van de AVG voorziene doorgifte-instrumenten in het kader van uw doorgiften ondermijnt. Wanneer u door uitsluitend een in artikel 46 van de AVG voorzien doorgifte-instrument te gebruiken, niet een in grote lijnen overeenkomend beschermingsniveau voor de doorgegeven gegevens kunt bereiken, kan deze leemte worden opgevuld met aanvullende maatregelen.

67. Wanneer u geen doeltreffende aanvullende maatregelen kunt vinden of uitvoeren om te verzekeren dat de doorgegeven gegevens in grote lijnen een overeenkomend beschermingsniveau genieten, moet u niet beginnen met het doorgeven van persoonsgegevens naar het betreffende derde land op basis van het door u gekozen doorgifte-instrument. Als u reeds gegevens doorgeeft, bent u verplicht de doorgifte van persoonsgegevens onmiddellijk op te schorten of te beëindigen.

68. De bevoegde toezichthoudende autoriteit heeft de bevoegdheid om doorgiften van persoonsgegevens naar het derde land op te schorten of te beëindigen als de bescherming van de doorgegeven gegevens die is vereist in het recht van de Unie, in het bijzonder artikel 45 en 46 van de AVG en het Handvest van de grondrechten, niet kan worden gewaarborgd.

Voor het Europees Comité voor gegevensbescherming

De voorzitter

(Andrea Jelinek)

[65] C-311/18 (Schrems II), punt 93.

BIJLAGE 1: DEFINITIES

- Onder “derde land” wordt verstaan: elk land dat geen lidstaat is van de EER.
- Onder “EER” wordt verstaan: de Europese Economische Ruimte. Deze omvat de lidstaten van de Europese Unie en IJsland, Noorwegen en Liechtenstein. Krachtens de EER-Overeenkomst, in het bijzonder bijlage XI en protocol 37 daarvan, is de AVG op deze laatste van toepassing.
- “AVG” verwijst naar 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).
- “Het Handvest” verwijst naar het Handvest van de grondrechten van de Europese Unie, PB C 326 van 26.10.2012, blz. 391.
- “HvJ-EU” of “het Hof” verwijst naar het Hof van Justitie van de Europese Unie. Het Hof is de gerechtelijke autoriteit van de Europese Unie en zorgt samen met de rechtbanken en gerechtshoven van de lidstaten voor de toepassing en de uniforme uitlegging van het recht van de Europese Unie.
- Onder “gegevensexporteur” wordt verstaan: de verwerkingsverantwoordelijke of verwerker binnen de EER die persoonsgegevens doorgeeft naar een verwerkingsverantwoordelijke of verwerker in een derde land.
- Onder “gegevensimporteur” wordt verstaan: de verwerkingsverantwoordelijke of verwerker in een derde land die vanuit de EER doorgegeven persoonsgegevens ontvangt of hier toegang toe krijgt.
- “In artikel 46 van de AVG voorzien doorgifte-instrument”: verwijst naar de in artikel 46 van de AVG voorziene passende waarborgen die gegevensexporteurs moeten instellen wanneer zij persoonsgegevens doorgeven naar een derde land waarvoor geen adequaatheidsbesluit is vastgesteld uit hoofde van artikel 45, lid 3, van de AVG. Artikel 46, leden 2 en 3, van de AVG bevatten de lijst van in artikel 46 van de AVG voorziene doorgifte-instrumenten waarvan verwerkingsverantwoordelijken en verwerkers gebruik mogen maken.
- Onder “standaardcontractbepalingen” wordt verstaan: standaardbepalingen inzake gegevensbescherming (of “modelcontractbepalingen”) die door de Europese Commissie zijn goedgekeurd voor het doorgeven van persoonsgegevens tussen verwerkingsverantwoordelijken of verwerkers in de EER en verwerkingsverantwoordelijken of verwerkers buiten de EER. Op grond van artikel 46, lid 2, onder c), en artikel 5, van de AVG, vormen de door de Europese Commissie goedgekeurde modelcontractbepalingen een doorgifte-instrument uit hoofde van de AVG.

BIJLAGE 2: VOORBEELDEN VAN AANVULLENDE MAATREGELEN

69. De volgende maatregelen zijn voorbeelden van aanvullende maatregelen die u kunt overwegen als u bent aangekomen bij stap 4 “Aanvullende maatregelen aannemen”. Deze lijst is niet uitputtend. Met het selecteren en uitvoeren van een of verschillende maatregelen is niet noodzakelijkerwijs en stelselmatig gewaarborgd dat uw doorgifte voldoet aan de norm voor een in grote lijnen overeenkomend beschermingsniveau zoals onder Unierecht is vereist. U moet de aanvullende maatregelen selecteren waarmee u op doeltreffende wijze dit beschermingsniveau voor uw doorgiften kunt waarborgen.

70. In de zin van het arrest van het HvJ-EU in de zaak Schrems II wordt een aanvullende maatregel slechts als doeltreffend beschouwd indien en voor zover deze betrekking heeft op de specifieke tekortkomingen die u hebt vastgesteld bij de beoordeling van de juridische situatie in het derde land. Indien u uiteindelijk niet een in grote lijnen overeenkomend beschermingsniveau kunt waarborgen, mogen de persoonsgegevens niet worden doorgegeven.

71. Mogelijk bent u als verwerkingsverantwoordelijke of verwerker al verplicht enkele van de in deze bijlage beschreven maatregelen uit te voeren, ook als uw gegevensimporteur onder een adequaatheidsbesluit valt, zoals u ook verplicht kunt worden deze uit te voeren wanneer u gegevens binnen de EER verwerkt.[66]

Technische maatregelen

72. In deze deel worden op niet-uitputtende wijze voorbeelden van technische maatregelen beschreven. Deze vormen een aanvulling op de waarborgen van de in artikel 46 van de AVG voorziene doorgifte-instrumenten, om te verzekeren dat bij doorgifte van persoonsgegevens naar een derde land wordt voldaan aan het krachtens Unierecht vereiste beschermingsniveau. Deze maatregelen zijn met name noodzakelijk wanneer het recht van dat land aan de gegevensimporteur verplichtingen oplegt die indruisen tegen de waarborgen van de in artikel 46 van de AVG voorziene doorgifte-instrumenten en die in het bijzonder afbreuk kunnen doen aan de contractuele waarborg van een in grote lijnen overeenkomend beschermingsniveau tegen de toegang van overheidsinstanties van dat derde land tot die gegevens[67].

73. Ter verduidelijking worden in dit deel eerst de technische maatregelen vermeld die in bepaalde scenario’s of praktijkvoorbeelden doeltreffend zouden kunnen zijn om een in grote lijnen overeenkomend beschermingsniveau te waarborgen. Vervolgens wordt ingegaan op enkele scenario’s of praktijkvoorbeelden waarin geen technische maatregelen konden worden gevonden om dit niveau van bescherming te waarborgen.

Scenario’s waarvoor *doeltreffende* maatregelen konden worden gevonden

74. De hieronder vermelde maatregelen zijn bedoeld om te verzekeren dat de toegang tot de doorgegeven gegevens door overheidsinstanties in derde landen geen afbreuk doet aan de doeltreffendheid van de

[66] Artikel 5, lid 2, van de AVG en artikel 32 van de AVG.
[67] C-311/18 (Schrems II), punt 135.

passende waarborgen zoals vervat in de in artikel 46 van de AVG voorziene doorgifte-instrumenten. Indien de toegang van de overheidsinstanties verder gaat dan hetgeen in een democratische samenleving noodzakelijk en evenredig is, zijn deze maatregelen van toepassing, ook wanneer een dergelijke toegang overeenkomstig het recht van het land van de importeur is[68]. Deze maatregelen zijn bedoeld om mogelijke inbreukmakende toegang uit te sluiten, doordat hiermee wordt voorkomen dat de autoriteiten de betrokkenen kunnen identificeren, informatie over hen kunnen afleiden, hen in een ander kader kunnen uitlichten of de doorgegeven gegevens kunnen koppelen aan andere gegevensreeksen die zij bezitten en waarin, naast andere gegevens, online-identificatiegegevens voorkomen die afkomstig zijn van apparaten, toepassingen, hulpmiddelen en protocollen die door betrokkenen in een ander kader zijn gebruikt.

75. Overheidsinstanties in derde landen kunnen proberen om toegang te krijgen tot doorgegeven gegevens

    a) tijdens de doorvoer, door zich toegang te verschaffen tot de communicatielijnen die worden gebruikt om de gegevens naar het ontvangende land over te brengen. Deze toegang kan passief zijn, waarbij de inhoud van de communicatie, mogelijk na een selectieproces, eenvoudigweg wordt gekopieerd. De toegang kan echter ook actief zijn, in de zin dat de overheidsinstanties ingrijpen in het communicatieproces door de inhoud niet alleen te lezen, maar ook te manipuleren of delen ervan achter te houden;

    b) tijdens de opslag door een bedoelde ontvanger van de gegevens, ofwel door zich toegang te verschaffen tot de verwerkingsinstallaties zelf of door een ontvanger van de gegevens te verplichten van belang zijnde gegevens op te sporen, aan de opslag te onttrekken en aan de autoriteiten over te dragen.

76. In dit deel wordt gekeken naar scenario's waarin maatregelen worden toegepast die in beide gevallen doeltreffend zijn. Indien het recht van het ontvangende land slechts voorziet in één soort toegang, kunnen er andere aanvullende maatregelen van toepassing zijn die voldoende zijn voor de specifieke situatie van een bepaalde doorgifte. Het is derhalve noodzakelijk dat de gegevensexporteur, met ondersteuning van de gegevensimporteur, zorgvuldig onderzoekt welke verplichtingen aan laatstgenoemde zijn opgelegd.

Zo geldt voor gegevensimporteurs in de Verenigde Staten die vallen onder 50 USC § 1881a (FISA 702), een rechtstreekse verplichting om toegang te verlenen tot de geïmporteerde gegevens die zij bezitten, bewaren of beheren, of om deze over te dragen. Dit geldt ook voor cryptografische sleutels die nodig zijn om de gegevens begrijpelijk te maken.

77. De scenario's hebben betrekking op specifieke omstandigheden en specifiek genomen maatregelen. Wijzigingen in de scenario's kunnen tot afwijkende conclusies leiden.

78. Ongeacht het beschermingsniveau dat wordt geboden in de voor de gegevensimporteur geldende wetgeving, moeten verwerkingsverantwoordelijken mogelijk enkele of alle hier beschreven maatregelen toepassen. In de concrete omstandigheden van de doorgifte zijn zij immers gehouden aan de artikelen 25 en 32 van de AVG. Met andere woorden kunnen exporteurs worden verplicht de in dit document beschreven maatregelen uit te voeren, ook als uw gegevensimporteur onder een

[68] Zie artikelen 47 en 52 van het Handvest van de grondrechten van de EU, artikel 23, lid 1, van de AVG en Aanbevelingen van het EDPB inzake Europese essentiële garanties voor surveillancemaatregelen.

adequaatheidsbesluit valt, zoals ook verwerkingsverantwoordelijken en verwerkers verplicht kunnen worden deze uit te voeren wanneer zij gegevens binnen de EER verwerken.

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

79. Een gegevensimporteur gebruikt een aanbieder van hostingdiensten in een derde land om persoonsgegevens op te slaan, bijvoorbeeld voor back-updoeleinden.

Indien

1. de persoonsgegevens voorafgaand aan de doorgifte worden verwerkt met behulp van sterke versleuteling;
2. het coderingsalgoritme en de bijbehorende parameters (b.v. lengte van de sleutel, werkwijze, indien van toepassing) voorzien zijn van de nieuwste technologie en geacht worden bestand te zijn tegen cryptoanalyse door de overheidsinstanties in het ontvangende land, waarbij rekening wordt gehouden met de middelen en de technische mogelijkheden (b.v. rekenkracht voor bruteforceaanvallen) waarover zij beschikken;
3. er bij de mate van versleuteling rekening is gehouden met het specifieke tijdvak gedurende welke de vertrouwelijkheid van de versleutelde persoonsgegevens moet worden bewaard;
4. het coderingsalgoritme zonder problemen is uitgevoerd door naar behoren onderhouden software waarvan de overeenstemming met de specificaties van het gekozen algoritme is gecontroleerd, b.v. middels certificering;
5. de sleutels op betrouwbare wijze worden beheerd (gegenereerd, bijgehouden, opgeslagen, waar van toepassing gekoppeld aan de identiteit van een beoogde ontvanger en ingetrokken), en
6. de sleutels uitsluitend worden bewaard en beheerd door de gegevensexporteur of andere entiteiten in de EER of een derde land, geografisch gebied of een of meer bepaalde sectoren binnen een derde land waaraan deze taak is toevertrouwd, of een internationale organisatie waarvoor de Commissie overeenkomstig artikel 45 van de AVG heeft vastgesteld dat een passend beschermingsniveau is gewaarborgd;

is het Comité van mening dat de uitgevoerde versleuteling in een doeltreffende aanvullende maatregel voorziet.

Praktijkvoorbeeld 2: Doorgifte van gepseudonimiseerde gegevens

80. Een gegevensexporteur pseudonimiseert eerst de gegevens die hij in bezit heeft en geeft deze vervolgens ter analyse door naar een derde land, bijvoorbeeld voor onderzoeksdoeleinden.

Indien

1. een gegevensexporteur de verwerkte persoonsgegevens op zodanige wijze doorgeeft dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld, noch

kunnen worden gebruikt om de betrokkene in een grotere groep eruit te lichten, zonder dat er aanvullende gegevens worden gebruikt[69],

2. die aanvullende gegevens uitsluitend in het bezit zijn van de gegevensexporteur en gescheiden worden bewaard in een lidstaat of in een derde land, geografisch gebied of een of meer bepaalde sectoren binnen een derde land, of bij een internationale organisatie waarvoor de Commissie overeenkomstig artikel 45 van de AVG heeft vastgesteld dat een passend beschermingsniveau is gewaarborgd,
3. verstrekking of onbevoegd gebruik van die aanvullende gegevens wordt voorkomen door passende technische en organisatorische waarborgen, de zekerheid bestaat dat de gegevensexporteur als enige controle heeft over het algoritme of het register waarmee de gegevens aan de hand van de aanvullende gegevens opnieuw kunnen worden geïdentificeerd, en
4. de verwerkingsverantwoordelijke, middels een gedegen analyse van de gegevens in kwestie en rekening houdend met mogelijke informatie die in het bezit is van de overheidsinstanties van het ontvangende land, heeft vastgesteld dat de gepseudonimiseerde persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon kunnen worden gekoppeld, zelfs niet als dergelijke informatie met de persoonsgegevens wordt samengevoegd en vergeleken,

is het Comité van mening dat de uitgevoerde pseudonimisering in een doeltreffende aanvullende maatregel voorziet.

81. Houd er rekening mee dat in veel situaties een natuurlijke persoon ook kan worden geïdentificeerd aan de hand van elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon, diens fysieke locatie of diens interactie op bepaalde tijdstippen met een internetdienst[70], zelfs als hun naam, adres en andere normale identificatiegegevens worden weggelaten.

82. Dit geldt met name wanneer de gegevens betrekking hebben op het gebruik van informatiediensten (tijdstip van toegang, volgorde van de geopende functies, kenmerken van het gebruikte apparaat enz.). Deze diensten kunnen, net als de importeur van persoonsgegevens, gebonden zijn aan de verplichting om dezelfde overheidsinstanties in hun rechtsgebied toegang te verlenen, waardoor de kans groot is dat deze vervolgens beschikken over gegevens over het gebruik van de betreffende informatiediensten door de persoon of de personen die zij op het oog hebben.

83. Gelet op het feit dat het gebruik van sommige informatiediensten openbaar van aard is, of deze worden geëxploiteerd door partijen die over aanzienlijke middelen beschikken, moeten verwerkingsverantwoordelijken extra zorgvuldigheid betrachten en er rekening mee houden dat overheidsinstanties in hun rechtsgebied waarschijnlijk beschikken over gegevens over het gebruik van informatiediensten door een persoon die zij op het oog hebben.

[69] In lijn met artikel 4, lid 5, van de AVG: "pseudonimisering": het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

[70] Artikel 4, lid 1, van de AVG: "persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatiegegeven zoals een naam, een identificatienummer, locatiegegevens, een online identificatiegegeven of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Praktijkvoorbeeld 3: Versleutelde gegevens met uitsluitend doorvoer in een derde land

84. Een gegevensexporteur wil gegevens doorgeven naar een bestemming die overeenkomstig artikel 45 van de AVG is erkend als passende bescherming biedend. De route van de gegevens loopt via een derde land.

Indien

1. een gegevensexporteur persoonsgegevens doorgeeft aan een gegevensimporteur in een rechtsgebied waar gepaste bescherming is verzekerd, de gegevens via het internet worden overgedragen en de geografische route van de gegevens mogelijk door een derde land loopt waar geen in grote lijnen overeenkomend beschermingsniveau wordt geboden,
2. tijdens het transport versleuteling wordt gebruikt waarvan is verzekerd dat de gebruikte coderingsprotocollen de nieuwste technologie bevatten en doeltreffend bescherming bieden tegen actieve en passieve aanvallen met middelen waarvan bekend is dat de overheidsinstanties van het derde land hierover beschikken,
3. ontcijfering uitsluitend mogelijk is buiten het derde land in kwestie,
4. de bij de communicatie betrokken partijen een betrouwbare certificeringsinstantie voor publieke sleutels of publiekesleutelinfrastructuur gebruiken,
5. er specifieke beschermende en technisch hoogstaande maatregelen tegen actieve en passieve aanvallen op de versleuteling tijdens transport worden gebruikt,
6. wanneer de versleuteling tijdens transport op zichzelf geen gepaste zekerheid biedt op grond van ervaringen met kwetsbaarheden in de gebruikte infrastructuur of software, de persoonsgegevens ook end-to-end op de applicatielaag met technisch hoogstaande versleutelingsmethoden zijn versleuteld,
7. het coderingsalgoritme en de bijbehorende parameters (b.v. lengte van de sleutel, werkwijze, indien van toepassing) voorzien zijn van de nieuwste technologie en geacht worden bestand te zijn tegen cryptoanalyse door de overheidsinstanties in het land van doorvoer, waarbij rekening wordt gehouden met de middelen en de technische mogelijkheden (b.v. rekenkracht voor bruteforceaanvallen) waarover zij beschikken;
8. er bij de mate van versleuteling rekening is gehouden met het specifieke tijdvak gedurende welke de vertrouwelijkheid van de versleutelde persoonsgegevens moet worden bewaard;
9. het coderingsalgoritme zonder problemen is uitgevoerd door naar behoren onderhouden software waarvan de overeenstemming met de specificaties van het gekozen algoritme is gecontroleerd, b.v. middels certificering;
10. er kan worden uitgesloten dat er achterdeurtjes (in hardware en software) aanwezig zijn,
11. de sleutels op betrouwbare wijze worden beheerd (gegenereerd, bijgehouden, opgeslagen, waar van toepassing gekoppeld aan de identiteit van de beoogde ontvanger en ingetrokken), door de exporteur of door een door de exporteur vertrouwde entiteit in een rechtsgebied waar een in grote lijnen overeenstemmend beschermingsniveau wordt geboden,

is het Comité van mening dat versleuteling tijdens transport, waar nodig in combinatie met end-to-end versleuteling van de inhoud, in een doeltreffende aanvullende maatregel voorziet.

Praktijkvoorbeeld 4: Beschermde ontvanger

85. Een gegevensexporteur geeft gegevens door aan een gegevensimporteur in een derde land die onder het recht van dat land specifieke bescherming geniet, b.v. met het oog op het gezamenlijk aanbieden van medische behandeling van een patiënt of juridische diensten voor een cliënt.

Indien

1. een in een derde land gevestigde gegevensimporteur op grond van het recht in dat land is gevrijwaard van mogelijke inbreukmakende toegang tot de gegevens die deze ontvanger voor het gegeven doel in bezit heeft, b.v. omdat er op de gegevensimporteur een geheimhoudingsplicht van toepassing is,
2. die vrijstelling ook geldt voor alle informatie in het bezit van de gegevensimporteur die mogelijk wordt gebruikt om de bescherming van vertrouwelijke informatie te omzeilen (cryptografische sleutels, wachtwoorden, andere aanmeldgegevens, enz.).
3. de gegevensimporteur de diensten van een verwerker niet gebruikt op een manier die de overheidsinstanties de mogelijkheid biedt toegang tot de gegevens te krijgen terwijl deze in het bezit van de verwerker zijn, en de gegevensimporteur de gegevens niet doorzendt naar een andere entiteit die niet is beschermd, op basis van de in artikel 46 van de AVG voorziene doorgifte-instrumenten,
4. de persoonsgegevens voorafgaand aan de verzending worden versleuteld met een van de laatste technologie voorziene methode die waarborgt dat de gegevens, gedurende de volledige tijd dat deze bescherming behoeven, niet gedecodeerd kunnen worden zonder de decoderingssleutel (end-to-end-versleuteling) te kennen,
5. de beschermde gegevensimporteur als enige de decoderingssleutel in bewaring heeft en deze op gepaste wijze is afgeschermd tegen onbevoegd gebruik of vrijgave, met technische en organisatorische maatregelen die voldoen aan de nieuwste technologische ontwikkelingen,
6. de gegevensexporteur op betrouwbare wijze heeft vastgesteld dat de coderingssleutel die hij voornemens is te gebruiken, overeenstemt met de coderingssleutel die in het bezit is van de ontvanger,

is het Comité van mening dat de versleuteling tijdens transport in een doeltreffende aanvullende maatregel voorziet.

Praktijkvoorbeeld 5: Gesplitste verwerking of verwerking door meerdere partijen

86. De gegevensexporteur wil dat persoonsgegevens gezamenlijk worden verwerkt door twee of meer onafhankelijke verwerkers in verschillende rechtsgebieden, zonder dat de inhoud van de gegevens aan hen bekend wordt gemaakt. Voorafgaand aan de verzending worden de gegevens zodanig gesplitst dat geen enkel deel dat een afzonderlijke verwerker ontvangt, toereikend is om alle of een deel van de persoonsgegevens te reconstrueren. De gegevensexporteur ontvangt afzonderlijk het resultaat van de verwerking van elk van de verwerkers en voegt de delen samen om tot een uiteindelijk resultaat te komen dat kan bestaan uit persoonsgegevens of geaggregeerde gegevens.

Indien

1. een gegevensexporteur persoonsgegevens op zodanige wijze verwerkt dat deze in twee of meer delen worden gesplitst die elk niet langer aan een specifieke betrokkene kunnen worden toegeschreven of toegekend zonder dat er aanvullende informatie wordt gebruikt,
2. elk deel wordt doorgegeven naar afzonderlijke verwerkers die in verschillende rechtsgebieden zijn bevestigd,
3. de verwerkers optioneel de gegevens gezamenlijk verwerken, bijvoorbeeld met behulp van veilige rekenmethoden voor meerdere partijen, op zodanige wijze dat aan geen van de partijen informatie wordt vrijgegeven waarover zij niet beschikten voordat de rekenmethoden werden uitgevoerd,
4. het bij de gedeelde rekenmethoden gebruikte algoritme is beveiligd tegen actieve vijanden,

5. er geen bewijs is voor samenwerking tussen de overheidsinstanties in de respectieve rechtsgebieden van de verwerkers, waardoor deze toegang krijgen tot alle reeksen persoonsgegevens die de verwerkers in bezit hebben en in staat zijn de inhoud van de persoonsgegevens op duidelijke wijze te reconstrueren en te gebruiken waar een dergelijk gebruik niet de essentie van de grondrechten en vrijheden van de betrokkenen eerbiedigt. Analoog hieraan mogen de overheidsinstanties van elk van beide landen niet beschikken over de bevoegdheid tot toegang tot persoonsgegevens die in het bezit zijn van verwerkers in alle betreffende rechtsgebieden,
6. de verwerkingsverantwoordelijke, middels een gedegen analyse van de gegevens in kwestie en rekening houdend met mogelijke informatie die in het bezit is van de overheidsinstanties van de ontvangende landen, heeft vastgesteld dat de aan de verwerkers verzonden delen persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon kunnen worden gekoppeld, zelfs niet als dergelijke informatie met de persoonsgegevens wordt vergeleken,

is het Comité van mening dat de uitgevoerde gesplitste verwerking in een doeltreffende aanvullende maatregel voorziet.

Scenario's waarvoor geen *doeltreffende* maatregelen konden worden gevonden

87. De hieronder voor bepaalde scenario's beschreven maatregelen zijn niet doeltreffend in het waarborgen van een in grote lijnen overeenkomend beschermingsniveau voor de naar het derde land doorgegeven gegevens. Zij komen dus niet in aanmerking als aanvullende maatregelen.

Praktijkvoorbeeld 6: Doorgifte naar aanbieders van clouddiensten of andere verwerkers waarvoor toegang tot ongecodeerde gegevens is vereist

88. Een gegevensexporteur gebruikt een aanbieder van clouddiensten of andere verwerker om, overeenkomstig zijn aanwijzingen in een derde land, persoonsgegevens te verwerken.

Indien

1. een verwerkingsverantwoordelijke gegevens naar een aanbieder van clouddiensten of andere verwerker doorgeeft,
2. de aanbieder van clouddiensten of andere verwerker voor het uitvoeren van de toegewezen opdracht toegang nodig heeft tot ongecodeerde gegevens, en
3. de aan de overheidsinstanties van het ontvangende land verleende bevoegdheid tot toegang tot de doorgegeven gegevens verder gaat dan hetgeen in een democratische samenleving noodzakelijk en evenredig is,[71]

kan het Comité, gezien de huidige staat van de techniek, geen doeltreffende technische maatregel bedenken om te voorkomen dat met die toegang inbreuk wordt gemaakt op de rechten van betrokkenen. Het Comité sluit niet uit dat door verdere ontwikkeling van de technologie maatregelen

[71] Zie artikelen 47 en 52 van het Handvest van de grondrechten van de EU, artikel 23, lid 1, van de AVG en Aanbevelingen van het EDPB inzake Europese essentiële garanties voor surveillancemaatregelen.

kunnen worden geboden waarmee de bedoelde commerciële doeleinden worden verwezenlijkt, zonder dat hiervoor ongecodeerde toegang is vereist.

89. In de gegeven scenario's, waarin het voor het verlenen van de dienst door de verwerker technisch gezien noodzakelijk is dat de persoonsgegevens niet worden versleuteld, vormen versleuteling tijdens transport en versleuteling van gegevens in ruste, zelfs als ze in combinatie worden toegepast, geen aanvullende maatregel waarmee een in grote lijnen overeenstemmend beschermingsniveau kan worden geboden als de gegevensimporteur in het bezit is van de cryptografische sleutels.

Praktijkvoorbeeld 7: Toegang tot gegevens op afstand voor commerciële doeleinden

90. Een gegevensexporteur stelt persoonsgegevens ter beschikking aan entiteiten in een derde land om deze te gebruiken voor gedeelde commerciële doeleinden. Een veel voorkomende constellatie kan bestaan uit een op het grondgebied van een lidstaat gevestigde verwerkingsverantwoordelijke of verwerker die persoonsgegevens doorgeeft naar een verwerkingsverantwoordelijke of verwerker in een derde land die tot hetzelfde concern behoort, of een groep ondernemingen die gezamenlijk bij een economische activiteit zijn betrokken. De gegevensimporteur kan de gegevens die hij ontvangt bijvoorbeeld gebruiken om aan de gegevensexporteur personeelsdiensten te verlenen, waarvoor hij personeelsgegevens nodig heeft, of om per telefoon of e-mail te communiceren met klanten van de gegevensexporteur die in de Europese Unie wonen.

Indien

1. een gegevensexporteur persoonsgegevens doorgeeft aan een gegevensimporteur in een derde land door deze in een gezamenlijk gebruikt informatiesysteem beschikbaar te stellen op een manier die de importeur de mogelijkheid biedt directe toegang tot gegevens naar eigen keuze te krijgen, of deze direct, afzonderlijk of in bulk, via gebruik van een communicatiedienst door te geven,
2. de importeur de ongecodeerde gegevens voor eigen doeleinden gebruikt,
3. de aan de overheidsinstanties van het ontvangende land verleende bevoegdheid tot toegang tot de doorgegeven gegevens verder gaat dan hetgeen in een democratische samenleving noodzakelijk en evenredig is,

kan het Comité geen doeltreffende technische maatregel bedenken om te voorkomen dat met die toegang inbreuk wordt gemaakt op de rechten van betrokkenen.

91. In de gegeven scenario's, waarin het voor het verlenen van de dienst door de verwerker technisch gezien noodzakelijk is dat de persoonsgegevens niet worden versleuteld, vormen versleuteling tijdens transport en versleuteling van gegevens in ruste, zelfs als ze in combinatie worden toegepast, geen aanvullende maatregel waarmee een in grote lijnen overeenstemmend beschermingsniveau kan worden geboden als de gegevensimporteur in het bezit is van de cryptografische sleutels.

Aanvullende contractuele maatregelen

92. Deze maatregelen bestaan in het algemeen uit unilaterale, bilaterale of multilaterale[72] contractuele verplichtingen.[73] Als een in artikel 46 voorzien doorgifte-instrument wordt gebruikt, zal dit in de meeste gevallen reeds een aantal (grotendeels contractuele) verplichtingen voor de gegevensexporteur en de gegevensimporteur bevatten, die zijn bedoeld om als waarborgen voor de persoonsgegevens te dienen.[74]

93. In bepaalde situaties waarin, de omstandigheden van de doorgifte in acht nemend, deze niet voldoen aan alle voorwaarden die zijn vereist om een beschermingsniveau te bieden dat in grote lijnen overeenkomt met het in de EU gewaarborgde beschermingsniveau, kunnen deze maatregelen de door de het doorgifte-instrument en de betreffende wetgeving in het derde land geboden waarborgen aanvullen en versterken. Gezien de aard van contractuele maatregelen, die in het algemeen de autoriteiten van dat land niet binden wanneer zij geen partij bij de overeenkomst zijn[75], moeten deze maatregelen met andere technische en organisatorische maatregelen worden gecombineerd om het vereiste beschermingsniveau te bieden. Met het selecteren en uitvoeren van een of verschillende maatregelen is niet noodzakelijkerwijs en stelselmatig gewaarborgd dat uw doorgifte voldoet aan de norm voor een in grote lijnen overeenkomend beschermingsniveau zoals onder Unierecht is vereist.

94. Afhankelijk van welke contractuele maatregelen reeds zijn opgenomen in het in artikel 46 van de AVG voorziene doorgifte-instrument dat u gebruikt, kunnen extra contractuele maatregelen ook nuttig zijn zodat in de EER gevestigde gegevensexporteurs zich bewust worden van nieuwe ontwikkelingen die van invloed zijn op de bescherming van naar derde landen doorgegeven gegevens.

95. Zoals gezegd, met contractuele maatregelen kan niet worden uitgesloten dat wetgeving van een derde land die niet voldoet aan de Europese essentiële garanties van het EDPB, wordt toegepast in die gevallen waarin de wetgeving de importeurs verplicht gehoor te geven wanneer zij door overheidsinstanties gelast worden gegevens die zij hebben ontvangen, bekend te maken.[76]

96. Hieronder worden enkele voorbeelden van deze mogelijke contractuele maatregelen genoemd, ingedeeld naar het soort maatregel:

[72] Bijvoorbeeld als onderdeel van bindende bedrijfsvoorschriften, waarin in elk geval enkele van de hieronder vermelde maatregelen moeten zijn geregeld.

[73] Deze zijn particulier van aard en mogen niet worden beschouwd als internationale overeenkomsten onder internationaal publiekrecht. Indien afgesloten met particuliere instanties in derde landen, zullen de overeenkomsten normaal gesproken de overheidsinstanties van het land niet kunnen binden aangezien die instanties geen partij zijn bij de overeenkomst, zoals het Hof in haar arrest in de zaak C-311/18 (Schrems II) in punt 125 heeft onderstreept.

[74] Zie het arrest in de zaak C-311/18 (Schrems II), punt 137, waarin het Hof hieruit voortvloeiend erkent dat de modelcontractbepalingen "doeltreffende mechanismen bevat[ten] waarmee in de praktijk kan worden gewaarborgd dat het door het Unierecht vereiste beschermingsniveau wordt geëerbiedigd en dat de doorgifte van persoonsgegevens op basis van dergelijke bepalingen wordt opgeschort of verboden ingeval die bepalingen worden geschonden of onmogelijk kunnen worden nageleefd"; zie ook punt 148).

[75] C-311/18 (Schrems II), punt 125.

[76] HvJ-EU, arrest in de zaak C-311/18 (Schrems II), punt 132.

Opname van de contractuele verplichting om bepaalde technische maatregelen te gebruiken

97. ***Afhankelijk van de specifieke omstandigheden van de doorgifte moet wellicht in het contract worden opgenomen dat doorgiften alleen mogen plaatsvinden als er bepaalde technische maatregelen zijn ingesteld (zie hierboven de voorgestelde technische maatregelen).***

98. ***Voorwaarden voor doeltreffendheid:***

- Deze bepaling kan doeltreffend zijn in situaties waarin de exporteur heeft vastgesteld dat er technische maatregelen nodig zijn. Dit zou dan op wettelijke wijze moeten worden vastgelegd om te verzekeren dat de importeur zich ook verbindt tot het instellen van technische maatregelen als dat nodig is.

Verplichtingen ten aanzien van transparantie:

99. ***De exporteur kan bijlagen bij het contract voegen met door de importeur naar beste vermogen verstrekte informatie over de toegang tot gegevens door overheidsinstanties, met inbegrip van het terrein van inlichtingendiensten, op voorwaarde dat de wetgeving in het land van bestemming voldoet aan de Europese essentiële garanties van het EDPB. Het kan de gegevensexporteur helpen te voldoen aan de verplichting om de beoordeling van het beschermingsniveau in het derde land te documenten.***

100. De importeur kan bijvoorbeeld worden verzocht om:

(1) een opsomming te geven van de op de importeur of zijn (sub)verwerkers toepasselijke wet- en regelgeving in het land van bestemming waarin de toegang van overheidsinstanties tot de gegevens van de doorgifte wordt toegestaan, in het bijzonder op het gebied van inlichtingendiensten, wetshandhaving en het administratief en regelgevend toezicht op de doorgegeven gegevens;
(2) bij ontstentenis van wetgeving die de toegang van overheidsinstanties tot gegevens regelt, informatie en statistieken te verstrekken op basis van de ervaring van de importeur of verslagen uit verschillende bronnen (b.v. partners, open bronnen, nationale rechtspraak en besluiten van toezichthoudende organen) over de toegang door overheidsinstanties tot persoonsgegevens in situaties waarvan hier sprake is (d.w.z. in het specifieke regelgevende gebied; gezien het soort entiteiten waar de gegevensimporteur toe behoort;...).
(3) aan te geven welke maatregelen zijn genomen om de toegang tot doorgegeven gegevens te voorkomen (indien van toepassing);
(4) in voldoende mate gedetailleerde informatie te verstrekken over alle verzoeken tot toegang tot persoonsgegevens van overheidsinstanties die de importeur in een bepaald tijdvak heeft ontvangen,[77] in het bijzonder op de hierboven onder 1) genoemde gebieden, met informatie over de ontvangen verzoeken, de gegevens waarom werd verzocht, de

[77] De duur van het tijdvak moet afhangen van het risico voor de rechten en vrijheden van de betrokkenen wier gegevens in de betreffende doorgifte worden doorgegeven, b.v. het jaar voorafgaand aan het afsluiten van het gegevensexportinstrument met de gegevensexporteur.

verzoekende instantie en de rechtsgrondslag voor bekendmaking en in hoeverre de importeur het gegevensverzoek bekend heeft gemaakt;[78]

(5) geef aan of en in hoeverre het de importeur wettelijk verboden is de hierboven onder (1) tot en met (5) genoemde informatie te verstrekken.

101. Deze informatie kan worden verstrekt in de vorm van gestructureerde vragenlijsten die de importeur invult en ondertekent, in combinatie met de contractuele verplichting dat de importeur elke mogelijke wijziging in deze informatie binnen een vastgestelde periode meldt, zoals momenteel de praktijk is bij zorgvuldigheidsprocedures.

102. ***Voorwaarden voor doeltreffendheid:***

- De importeur moet in staat zijn dit soort informatie naar beste vermogen en naar beste vermogen aan de exporteur te verstrekken.[79]

- Deze aan de importeur opgelegde verplichting is een manier om ervoor te zorgen dat de exporteur zich bewust wordt en blijft van de risico's die aan een gegevensdoorgifte naar een derde land zijn verbonden. Hierdoor heeft de exporteur de mogelijkheid van het sluiten van de overeenkomst af te zien of, als de informatie wijzigt nadat de overeenkomst is afgesloten, te voldoen aan zijn verplichting om de doorgifte op te schorten en/of de overeenkomst te beëindigen als het recht in het derde land, de waarborgen van de in artikel 46 voorziene doorgifte-instrumenten en mogelijke extra waarborgen die zijn aangenomen, niet langer een beschermingsniveau kunnen bieden dat in grote lijnen overeenkomt met het niveau in de EU. Deze verplichting kan echter geen rechtvaardiging vormen voor het bekendmaken van persoonsgegevens door de importeur, noch aanleiding geven tot de verwachting dat er geen verdere verzoeken tot toegang zullen zijn.

***

103. ***De exporteur kan ook bepalingen toevoegen op grond waarvan de importeur verklaart dat 1) hij niet willens en wetens achterdeurtjes of vergelijkbare programmering heeft aangebracht die kunnen worden gebruikt om toegang te krijgen tot het systeem en/of persoonsgegevens, 2) hij niet willens en wetens bedrijfsprocessen heeft gecreëerd of gewijzigd op een wijze die de toegang tot persoonsgegevens of systemen vergemakkelijkt, en 3) het nationale recht of het overheidsbeleid de importeur niet verplichten achterdeurtjes aan te brengen of te handhaven of de toegang tot persoonsgegevens of systemen te faciliteren of als importeur in het bezit te zijn van de coderingssleutel of deze over te dragen.[80]***

104. ***Voorwaarden voor doeltreffendheid:***

- Als er wetgeving of overheidsbeleid bestaat op grond waarvan het de importeur niet is toegestaan deze informatie bekend te maken, is deze bepaling niet langer doeltreffend. De

[78] Het vervullen van deze taak is als zodanig niet voldoende om een gepast beschermingsniveau te bieden. Tegelijkertijd maakt elke niet-passende bekendmaking die daadwerkelijk heeft plaatsgevonden, het noodzakelijk om aanvullende maatregelen uit te voeren.

[79] Zie punt 32, lid 5, hierboven.

[80] Deze bepaling is belangrijk om een gepast beschermingsniveau voor de doorgegeven persoonsgegevens te waarborgen en zou meestal verplicht moeten worden gesteld.

importeur kan de overeenkomst dan niet aangaan of moet de exporteur ervan op de hoogte stellen dat hij niet in staat is te blijven voldoen aan zijn contractuele verplichtingen.[81]

- Voor die gevallen waarin de importeur niet heeft aangegeven dat er een achterdeur of vergelijkbare programmering, gemanipuleerde bedrijfsprocessen of een verplichting tot het uitvoeren van een van deze zaken bestaat, of de exporteur niet onmiddellijk informeert zodra hij van het bestaan hiervan kennisneemt, moeten in de overeenkomst sancties en/of de mogelijkheid voor de exporteur om de overeenkomst op korte termijn te beëindigen, worden opgenomen.

***

105. ***Bij het uitvoeren van controles[82] of inspecties van de gegevensverwerkingsinstallaties van de importeur, ter plaatse en/of op afstand, om te controleren of er gegevens aan overheidsinstanties bekend zijn gemaakt en onder welke voorwaarden (toegang die niet verder gaat dan hetgeen in een democratische samenleving noodzakelijk en evenredig is), kan de exporteur zijn positie versterken door bijvoorbeeld een korte termijn voor kennisgeving en mechanismen voor een snel optreden van controleorganen op te nemen en de autonomie van de exporteur in de keuze van de controleorganen te versterken.***

106. ***Voorwaarden voor doeltreffendheid:***

- Om volledig doeltreffend te zijn, moet de juridische en technische reikwijdte van de controle alle verwerkingsactiviteiten omvatten die de verwerkers of subverwerkers van de importeur uitvoeren op de in het derde land overgedragen persoonsgegevens.
- Vastleggingen van toegang en andere soortgelijke sporen moeten beschermd zijn tegen manipulatie zodat de controleurs kunnen zien of er gegevens zijn vrijgegeven. In vastleggingen van toegang en andere soortgelijke sporen moet ook onderscheid worden gemaakt tussen toegang voor reguliere bedrijfsactiviteiten en toegang op grond van bevelen of verzoeken tot toegang.

***

107. ***Wanneer er een eerste beoordeling van het recht en de praktijk van het derde land van de importeur is uitgevoerd en is gebleken dat deze aan de door de exporteur doorgegeven gegevens een beschermingsniveau bieden dat in grote lijnen overeenkomt met het in de EU geboden niveau, kan de exporteur nog steeds de verplichting van de gegevensimporteur om de gegevensexporteur onverwijld op de hoogte te stellen wanneer hij niet aan de contractuele verplichtingen, en dus ook niet aan de vereiste norm voor een "in grote lijnen overeenkomend gegevensbeschermingsniveau", kan voldoen, versterken.[83].***

[81] Zie punt 32, lid 5, hierboven.

[82] Zie bijvoorbeeld bepaling 5, onder f), van Besluit 2010/87/EU inzake modelcontractbepalingen tussen verwerkingsverantwoordelijken en verwerkers, waarin is bepaald dat controles ook kunnen plaatsvinden binnen het kader van een gedragscode of middels certificering.

[83] Bepaling 5, onder a), en onder d), i), van Besluit 2010/87/EU inzake modelcontractbepalingen.

108. Dit onvermogen om de modelcontractbepalingen na te leven, kan voortkomen uit wijzigingen in het recht of de praktijk van het derde land.[84] In de bepalingen kunnen specifieke en strenge tijdslimieten en procedures worden vastgesteld voor de snelle opschorting van de doorgifte van gegevens en/of de beëindiging van de overeenkomst en het terugzenden of verwijderen van de ontvangen gegevens door de importeur. Door bij te houden welke verzoeken er worden ontvangen, wat de reikwijdte daarvan is en in hoeverre de daartegen genomen maatregelen doeltreffend zijn, beschikt de exporteur over voldoende aanwijzingen om zijn verplichting om de doorgifte op te schorten of te beëindigen en/of de overeenkomst te beëindigen, uit te oefenen.

109. ***Voorwaarden voor doeltreffendheid:***

- De kennisgeving moet plaatsvinden voordat de toegang tot de gegevens wordt verleend. Gebeurt dit niet, dan zijn de rechten van de persoon mogelijk al geschonden tegen de tijd dat de exporteur de kennisgeving ontvangt, als het verzoek is gebaseerd op wetgeving van dat derde land die verder gaat dan hetgeen op grond van het uit hoofde van Unierecht verleende gegevensbeschermingsniveau is toegestaan. De kennisgeving kan nog steeds nuttig zijn om toekomstige schendingen te voorkomen en de exporteur in staat te stellen te voldoen aan zijn verplichting om de doorgifte van persoonsgegevens naar het derde land op te schorten en/of de overeenkomst te beëindigen.
- De gegevensimporteur moet de juridische en beleidsmatige ontwikkelingen volgen die ertoe kunnen leiden dat hij niet aan zijn verplichtingen kan voldoen en de gegevensexporteur onverwijld in kennis stellen van deze wijzigingen en ontwikkelingen, zo mogelijk voordat deze ten uitvoer worden gelegd, om de gegevensexporteur in staat te stellen de gegevens van de gegevensimporteur terug te halen.
- In de bepalingen moet een snel uit te voeren mechanisme worden opgenomen waarbij de gegevensexporteur de gegevensimporteur toestemming verleent om onverwijld de gegevens te beveiligen of terug te zenden naar de gegevensexporteur of, indien dit niet haalbaar is, de gegevens te verwijderen of veilig te versleutelen, zonder dat hij, indien is voldaan aan een bepaalde tussen de gegevensexporteur en gegevensimporteur overeengekomen drempel, hiervoor aanwijzingen van de exporteur hoeft af te wachten. De importeur moet dit mechanisme bij aanvang van de gegevensdoorgifte uitvoeren en dit regelmatig testen om te verzekeren dat het op korte termijn kan worden toegepast.
- Andere bepalingen kunnen de exporteur in staat stellen door middel van controles, inspecties en andere controlemaatregelen toe te zien op de naleving van deze verplichtingen door de importeur en deze af te dwingen met boeten voor de importeur en/of de mogelijkheid voor de exporteur om de doorgifte op te schorten en/of onmiddellijk de overeenkomst te beëindigen.

***

[84] Zie C-311/18 (Schrems II), punt 139 waarin het Hof stelt: "Voorts biedt bepaling 5, onder d), i), de ontvanger van de doorgifte van persoonsgegevens weliswaar de mogelijkheid om, in geval van een wettelijk verbod, zoals een strafrechtelijk verbod dat ten doel heeft de vertrouwelijkheid van een wetshandhavingsonderzoek te bewaren, de verwerkingsverantwoordelijke niet in kennis te stellen van een juridisch bindend verzoek van een wetshandhavingsinstantie om verstrekking van persoonsgegevens, maar is hij overeenkomstig bepaling 5, onder a), van de bijlage bij het MCB-besluit niettemin ertoe verplicht om de verwerkingsverantwoordelijke in kennis te stellen van het feit dat hij er niet toe in staat is te voldoen aan de standaardbepalingen inzake gegevensbescherming."

110. ***Voor zover toegestaan in het nationale recht van het derde land kunnen in de overeenkomst zwaardere verplichtingen ten aanzien van transparantie van de importeur worden opgenomen middels de zogenoemde "Warrant Canary"-methode, waarbij de importeur zich ertoe verbindt regelmatig (b.v. ten minste elke 24 uur) een cryptografisch ondertekend bericht te publiceren waarin aan de exporteur wordt gemeld dat er tot een bepaalde datum en een bepaald tijdstip geen bevel tot bekendmaking van persoonsgegevens of soortgelijk verzoek is ontvangen. Indien een bijgewerkte versie van deze kennisgeving uitblijft, is dit een aanwijzing voor de exporteur dat de importeur wellicht een bevel heeft ontvangen.***

111. ***Voorwaarden voor doeltreffendheid:***

- In de regelgeving van het derde land moet het verstrekken van deze vorm van passieve kennisgevingen door de importeur aan de exporteur zijn toegestaan.
- De "warrant-canary"-meldingen moet door de gegevensexporteur automatisch worden gevolgd.
- De gegevensimporteur moet verzekeren dat zijn privésleutel voor het ondertekenen van de kennisgevingen veilig wordt bewaard en dat hij niet kan worden gedwongen om op grond van de regelgeving in het derde land valse kennisgevingen uit te geven. Hiervoor kan het nuttig zijn dat er meerdere handtekeningen van verschillende personen nodig zijn en/of dat de kennisgevingen worden uitgegeven door een persoon die zich buiten het rechtsgebied van het derde land bevindt.

Verplichtingen tot het nemen van specifieke maatregelen

112. ***De importeur kan zich ertoe verbinden in de wetgeving van het land van bestemming de rechtmatigheid van een bevel tot bekendmaking van gegevens na te gaan, met name of dit binnen de aan de verzoekende overheidsinstantie toegekende bevoegdheden blijft, en het bevel aan te vechten als na zorgvuldige beoordeling blijkt dat er krachtens het recht van het land van bestemming gronden bestaan om dit te doen. Wanneer een gegevensimporteur het bevel aanvecht, moet hij verzoeken om tijdelijke maatregelen waarmee de gevolgen van het bevel worden opgeschort totdat de rechtbank een besluit heeft genomen over de gegrondheid van het bevel. De importeur is verplicht de gevraagde persoonsgegevens pas bekend te maken wanneer hij uit hoofde van het toepasselijke procesrecht hiertoe is verplicht. De gegevensimporteur verbindt zich tevens ertoe om, wanneer hij gehoor geeft aan het bevel, de minimaal toegestane hoeveelheid informatie te verstrekken, op basis van een redelijke uitlegging van het bevel.***

113. ***Voorwaarden voor doeltreffendheid:***

- Het wettelijk bevel van het derde land moet doeltreffende juridische wegen bieden om bevelen tot het vrijgeven van gegevens aan te vechten.
- De met deze bepaling geboden extra bescherming zal altijd zeer beperkt zijn, aangezien een bevel tot het vrijgeven van gegevens weliswaar rechtmatig kan zijn uit hoofde van de rechtsorde van het derde land, maar deze rechtsorde wellicht niet voldoet aan de EU-normen. Noodzakelijkerwijs moet deze contractuele maatregel altijd in aanvulling op andere aanvullende maatregelen worden toegepast.
- Het recht van het derde land moet erin voorzien dat de aangevochten bevelen een opschortende werking hebben. Anders hebben de overheidsinstanties nog steeds toegang tot de gegevens van de persoon en wordt het effect van een mogelijke hieruit voortvloeiende

maatregel ten gunste van de persoon beperkt tot de mogelijkheid om schadevergoeding te eisen voor de negatieve gevolgen van het vrijgeven van de gegevens.
- Om aan deze verplichting te voldoen, moet de importeur naar beste vermogen de genomen maatregelen documenteren en voor de exporteur aantonen.

***

114. ***Net als in de hierboven beschreven situatie kan de importeur zich ertoe verbinden de verzoekende overheidsinstantie ervan in kennis te stellen dat het bevel onverenigbaar is met de waarborgen zoals vervat in het in artikel 46 van de AVG voorziene doorgifte-instrument[85] en de conflicterende verplichtingen die dat voor de importeur met zich meebrengt. Gelijktijdig en zo spoedig mogelijk stelt de importeur de exporteur en/of de bevoegde toezichthoudende autoriteit in de EER hiervan in kennis, voor zover dit overeenkomstig de rechtsorde van het derde land mogelijk is.***

115. ***Voorwaarden voor doeltreffendheid:***

- Dergelijke informatie over de in de EU-wetgeving verleende bescherming en de conflicterende verplichtingen moet in de rechtsorde van het derde land in enige mate juridische gevolgen hebben, zoals het vanuit juridisch of administratief oogpunt opnieuw beoordelen van een bevel of verzoek tot toegang, de vereiste van een gerechtelijk bevel en/of een tijdelijke opschorting van de doorgifte om de bescherming van de gegevens te verbeteren.
- De rechtsorde van het land mag de importeur niet ervan weerhouden de exporteur of ten minste de bevoegde toezichthoudende autoriteit in de EER van het ontvangen bevel of verzoek tot toegang in kennis te stellen.
- Om aan deze verplichting te voldoen, moet de importeur naar beste vermogen de genomen maatregelen documenteren en voor de exporteur aantonen.

Betrokkenen de mogelijkheid bieden hun rechten uit te oefenen.

116. ***In de overeenkomst kan worden opgenomen dat de toegang tot in platte tekst verzonden persoonsgegevens bij een normale gang van zaken (waaronder in ondersteuningssituaties) uitsluitend is toegestaan na uitdrukkelijke of impliciete toestemming van de exporteur en/of de betrokkene.***

117. ***Voorwaarden voor doeltreffendheid:***

- Deze bepaling kan doeltreffend zijn in situaties waarin importeurs van overheidsinstanties het verzoek ontvangen om op vrijwillige basis mee te werken, in tegenstelling tot bijvoorbeeld de toegang tot gegevens door overheidsinstanties die plaatsvindt zonder dat de importeur hiervan op de hoogte is of tegen diens wil.

[85] In de modelcontractbepalingen is bijvoorbeeld bepaald dat het verwerken van gegevens, met inbegrip van het doorgeven ervan, is en zal blijven worden uitgevoerd overeenkomstig "het toepasselijke recht inzake gegevensbescherming". Onder dit recht wordt verstaan "de wetgeving inzake de bescherming de grondrechten en vrijheden van personen en in het bijzonder het recht op privacy in verband met de verwerking van persoonsgegevens zoals van toepassing op een gegevensverwerkingsverantwoordelijke in de lidstaat waarin de gegevensexporteur is gevestigd." Het HvJ-EU bevestigt dat de bepalingen van de AVG, gelezen in het licht van het Handvest van de grondrechten van de EU, onderdeel uitmaken van die wetgeving, zie HvJ-EU C-311/18 (Schrems II), punt 138.

- In sommige situaties bevindt de betrokkene zich mogelijk niet in de positie om tegen de toegang bezwaar te maken of zijn toestemming te geven op een manier die voldoet aan alle voorwaarden zoals bepaald in het EU-recht (uit vrije wil verstrekt, specifiek, geïnformeerd en ondubbelzinnig) (b.v. in het geval van werknemers).[86]
- Deze bepaling is niet langer doeltreffend als het de importeur op grond van nationale regelgeving of beleid niet is toegestaan het bevel tot toegang bekend te maken, tenzij de bepaling wordt ondersteund met technische methoden die tussenkomst van de exporteur of de betrokkene voor toegang tot de gegevens in platte tekst vereisen. Dergelijke toegangsbeperkende technische maatregelen kunnen met name worden overwogen als er uitsluitend in specifieke ondersteunings- of onderhoudssituaties toegang wordt verleend, maar de gegevens zelf in de EER worden bewaard.

***

118. ***In de overeenkomst kan de importeur en/of de exporteur worden verplicht de betrokkene onverwijld in kennis te stellen van het van de overheidsinstanties van het derde land ontvangen bevel of verzoek, of van het feit dat de importeur niet aan zijn verplichtingen kan voldoen, om de betrokkene in staat te stellen om informatie te verzoeken en doelmatig verhaal te halen (b.v. door een vordering in te dienen bij zijn/haar bevoegde toezichthoudende autoriteit en/of gerechtelijke autoriteit en zijn/haar positie in de rechtbanken van het derde land kenbaar te maken).***

119. ***Voorwaarden voor doeltreffendheid:***

- Met deze kennisgeving kan de betrokkene worden gewaarschuwd in geval van mogelijke toegang tot zijn/haar gegevens door overheidsinstanties in derde landen. Die biedt de betrokkene de mogelijkheid om de exporteurs om aanvullende informatie te verzoeken en bij zijn/haar bevoegde toezichthoudende autoriteit een vordering in te stellen. Met deze bepaling kunnen ook enkele van de moeilijkheden worden weggenomen waar de persoon tegenaan loopt wanneer hij/zij zijn/haar positie *(locus standi)* voor de rechtbanken van het derde land moet aantonen om de toegang door overheidsinstanties tot zijn/haar gegevens aan te vechten.
- Er kan nationale regelgeving en beleid zijn die deze kennisgeving aan de betrokkene in de weg staan. Desondanks kunnen de exporteur en de importeur zich ertoe verbinden de betrokkene in kennis te stellen zodra de beperkingen op het verstrekken van gegevens worden opgeheven en hun uiterste best te doen om voor het verbod op vrijgave vrijstelling te verkrijgen. Minimaal kan worden bepaald dat de exporteur of de bevoegde toezichthoudende autoriteit de betrokkene in kennis stellen van de opschorting of beëindiging van de doorgifte van zijn/haar persoonsgegeven op grond van het feit dat de importeur, vanwege de ontvangst van een verzoek tot toegang, niet aan zijn contractuele verplichtingen kan voldoen.

***

120. ***In het contract kunnen de exporteur en de importeur worden verplicht de betrokkene bij te staan in de uitoefening van zijn/haar rechten in het rechtsgebied van het derde land door middel van ad-hoc verhaalmiddelen en juridisch advies.***

[86] Artikel 4, lid 11, van de AVG.

121. ***Voorwaarden voor doeltreffendheid:***

- In nationale regelgeving en beleid kunnen voorwaarden zijn opgelegd die de doeltreffendheid van de geboden ad-hoc verhaalmiddelen ondermijnen.
- Juridisch advies kan nuttig zijn voor de betrokkene, met name gelet op hoe complex en kostbaar het voor een betrokkene kan zijn om inzicht te krijgen in de rechtsorde van een derde land en vanuit het buitenland en mogelijk in een andere taal, juridische procedures in te stellen. De met deze bepaling geboden extra bescherming zal echter altijd beperkt zijn, aangezien het bieden van bijstand en juridisch advies op zich niet kunnen verhelpen dat de rechtsorde van een derde land niet voorziet in een beschermingsniveau dat in grote lijnen overeenkomt met het in de EU gewaarborgde niveau. Noodzakelijkerwijs moet deze contractuele maatregel altijd in aanvulling op andere aanvullende maatregelen worden toegepast.

Deze aanvullende maatregel is uitsluitend doeltreffend wanneer het recht van het derde land verhaalmogelijkheden bij de nationale rechtbanken biedt of er een ad-hoc verhaalmechanisme bestaat. Dit is echter in ieder geval geen efficiënte aanvullende maatregel tegen surveillancemaatregelen als er geen verhaalmechanisme bestaat.

Organisatorische maatregelen

122. Aanvullende organisatorische maatregelen kunnen bestaan uit interne beleidsmaatregelen, organisatorische werkwijzen en normen die verwerkingsverantwoordelijken voor zichzelf toepassen en opleggen aan de importeurs van gegevens in derde landen. Deze kunnen bijdragen aan het bieden van een coherente bescherming van persoonsgegevens gedurende de volledige verwerkingscyclus. Organisatorische maatregelen kunnen er ook aan bijdragen dat de exporteur zich beter bewust is van het risico op en de pogingen om toegang te verkrijgen tot de gegevens in derde landen en daar beter op kan reageren. Met het selecteren en uitvoeren van een of verschillende maatregelen is niet noodzakelijkerwijs en stelselmatig gewaarborgd dat uw doorgifte voldoet aan de norm voor een in grote lijnen overeenkomend beschermingsniveau zoals onder Unierecht is vereist. Afhankelijk van de specifieke omstandigheden van de doorgifte en de uitgevoerde beoordeling van de wetgeving van het derde land, zijn organisatorische maatregelen nodig als aanvulling op contractuele en/of technische maatregelen om te verzekeren dat het beschermingsniveau van de persoonsgegevens in grote lijnen overeenkomt met het in de EU gewaarborgde niveau.

123. Van geval tot geval moet worden beoordeeld welke maatregelen het meest geschikt zijn, waarbij rekening moet worden gehouden met de noodzaak voor verwerkingsverantwoordelijken en verwerkers om het beginsel van verantwoordingsplicht te eerbiedigen. Hieronder geeft het Comité enkele voorbeelden van organisatorische maatregelen die de exporteurs kunnen instellen. Deze lijst is niet uitputtend en er kunnen ook andere maatregelen zijn.

Intern beleid voor het beheer van doorgiften, met name bij groepen ondernemingen.

124. ***Vaststelling van toereikende interne beleidsmaatregelen met een duidelijke toekenning van verantwoordelijkheden bij doorgiften, rapportagekanalen en standaard bedrijfsprocedures voor infiltratieoperaties of officiële verzoeken van overheidsinstanties voor toegang tot de gegevens. Met name bij doorgiften tussen groepen ondernemingen kunnen deze beleidsmaatregelen onder meer bestaan uit het aanstellen van een speciaal team, dat binnen de EER moet zijn gevestigd en moet***

bestaan uit deskundigen op het gebied van IT, gegevensbescherming en privacywetgeving, voor de behandeling van verzoeken die betrekking hebben op vanuit de EU doorgegeven gegevens; het in kennis stellen van de leidinggevenden op het gebied van juridische zaken en bedrijfsvoering en van de gegevensimporteur na het ontvangen van dergelijke verzoeken; de procedurele stappen voor het aanvechten van onevenredige en onrechtmatige verzoeken en het verstrekken van transparante informatie aan betrokkenen.

125. Het ontwikkelen van een speciaal opleidingstraject voor personeel dat is belast met het beheren van verzoeken van overheidsinstanties tot toegang tot persoonsgegevens. Dit moet periodiek worden geactualiseerd op basis van nieuwe ontwikkelingen in de wetgeving en de rechtsspraak in de het derde land en in de EER. Tijdens de opleiding moet onder meer worden ingegaan op de vereisten in het EU-recht voor de toegang door overheidsinstanties tot persoonsgegevens, met name zoals deze voortvloeien uit artikel 52, lid 1, van het Handvest van grondrechten. Het bewustzijn van het personeel moet met name worden verhoogd aan de hand van de beoordeling van praktijkvoorbeelden van verzoeken van overheidsinstanties tot gegevenstoegang en door bij dergelijke praktijkvoorbeelden de uit artikel 52, lid 1, van het Handvest van grondrechten voortvloeiende norm toe te passen. Tijdens zo'n opleiding moet rekening worden gehouden met de specifieke situatie van de gegevensimporteur, d.w.z. de voor de gegevensimporteur toepasselijke wet- en regelgeving van het derde land, en waar mogelijk moet de opleiding in samenwerking met de gegevensexporteur worden ontwikkeld.

126. ***Voorwaarden voor doeltreffendheid:***

- Deze beleidsmaatregelen kunnen uitsluitend worden overwogen in die gevallen waarin het verzoek van overheidsinstanties in het derde land verenigbaar is met de EU-wetgeving.[87] Indien het verzoek niet hiermee verenigbaar is, zouden deze beleidsmaatregelen niet volstaan om de persoonsgegevens een in grote lijnen overeenkomend beschermingsniveau te bieden en moeten, zoals hierboven gesteld, de doorgiften worden stopgezet of moeten er gepaste aanvullende maatregelen ter voorkoming van de toegang worden ingesteld.

Maatregelen ten aanzien van transparantie en verantwoording

127. ***Documentatie en registratie van de verzoeken tot toegang die zijn ontvangen van overheidsinstanties en de gegeven reactie, en van de juridische argumentatie en de betrokken actoren (b.v. of de exporteur in kennis is gesteld en wat deze hierop heeft geantwoord, de beoordeling door het team dat is belast met de behandeling van dergelijke verzoeken, enz.). Dit register moet ter beschikking worden gesteld van de gegevensexporteur, die dit op zijn beurt kan doorgeven aan de betreffende betrokkenen wanneer dit is vereist.***

128. ***Voorwaarden voor doeltreffendheid:***

- In het derde land kan wetgeving bestaan die de bekendmaking van de verzoeken of van wezenlijke informatie daarin in de weg staat, waardoor deze praktijk niet langer doeltreffend is. De gegevensimporteur moet de exporteur in kennis stellen van zijn onvermogen om dergelijke documenten en registers te verstrekken en de exporteur daarmee de mogelijkheid bieden de doorgiften op te schorten als dergelijk onvermogen leidt tot een lager beschermingsniveau.

[87] Zie het arrest in de zaak C-362/14 (Schrems I), punt 94; C-311/18 (Schrems II), punten 168, 174, 175 en 176.

***

129. ***Regelmatige publicatie van transparantieverslagen of -overzichten met betrekking tot overheidsverzoeken voor toegang tot gegevens en op welke wijze hierop is gereageerd, voor zover publicatie in het lokaal recht is toegestaan.***

130. ***Voorwaarden voor doeltreffendheid:***

- De verstrekte informatie moet relevant, duidelijk en zo uitvoerig mogelijk zijn. In het derde land kan wetgeving bestaan die het verstrekken van uitvoerige informatie in de weg staat. In die gevallen moet de gegevensexporteur naar beste vermogen statistische gegevens of een vergelijkbaar soort geaggregeerde gegevens publiceren.

Maatregelen ten aanzien van de werkwijze van de organisatie en gegevensminimalisering

131. ***Reeds uit hoofde van het verantwoordingsbeginsel bestaande organisatorische voorschriften, zoals het toepassen van strikte en gefragmenteerde toegang tot gegevens en beleid en beste praktijken voor geheimhouding, op basis van een strikte toepassing van het "need-to-know"-beginsel, toezicht met regelmatige controles en handhaving via disciplinaire maatregelen, kunnen in het kader van een doorgifte eveneens nuttige maatregelen zijn. In dit verband moet worden overwogen de gegevens te minimaliseren, zodat de blootstelling van persoonsgegevens aan ongeautoriseerde toegang wordt beperkt. Zo kan het in bepaalde gevallen niet nodig zijn bepaalde gegevens door te geven (b.v. in het geval van toegang op afstand tot EER-gegevens, zoals in ondersteuningssituaties, wanneer in plaats van volledige toegang beperkte toegang wordt verleend; of wanneer voor de verlening van een dienst slechts de doorgifte van een beperkte reeks gegevens nodig is en niet van de volledige database).***

132. ***Voorwaarden voor doeltreffendheid:***

- Er moet voorzien zijn in regelmatige controles en disciplinaire maatregelen om de naleving van de maatregelen voor gegevensminimalisering ook in het kader van doorgiften te bewaken en af te dwingen.
- De gegevensexporteur moet, voordat de doorgifte plaatsvindt, een beoordeling uitvoeren van de persoonsgegevens die hij bezit, om vast te stellen welke gegevensreeksen gelet op het doel van de doorgifte niet noodzakelijk zijn en derhalve niet met de gegevensimporteur worden gedeeld.
- Om te verzekeren dat gegevens niet het voorwerp worden van ongeautoriseerde toegang, moeten de maatregelen voor gegevensminimalisering gepaard gaan met technische maatregelen. Zo kan bijvoorbeeld het uitvoeren van veilige, door meerdere partijen te gebruiken rekenmechanismen en het spreiden van versleutelde gegevensreeksen onder verschillende vertrouwde entiteiten, door de manier waarop dit is opgezet, voorkomen dat een unilaterale toegang tot het vrijgeven van identificeerbare gegevens leidt.

***

133. ***Ontwikkeling van beste praktijken om op gepaste en tijdige wijze de functionaris voor gegevensbescherming, voor zover aanwezig, en de juridische en interne controlediensten voor kwesties die betrekking hebben op internationale doorgiften van persoonsgegevens, te betrekken en hen toegang tot de informatie te geven.***

134. ***Voorwaarden voor doeltreffendheid:***

- De functionaris voor gegevensbescherming, voor zover aanwezig, en de juridische en interne controleteams moeten voorafgaand aan de doorgifte van alle relevante informatie worden voorzien. Hen moet om advies worden gevraagd inzake de noodzaak van de doorgifte en de eventuele extra waarborgen.
- De relevante informatie moet bijvoorbeeld bestaan uit de beoordeling van de noodzaak van de doorgifte van de specifieke persoonsgegevens, een overzicht van de toepasselijke wetgeving van het derde land en de waarborgen die de importeur heeft toegezegd uit te voeren.

Vaststelling van normen en beste praktijken

135. ***Vaststelling van strikte beleidsmaatregelen voor de beveiliging en privacy van gegevens, op basis van EU-certificering, gedragscodes of internationale normen (b.v. ISO-normen) en beste praktijken (b.v. ENISA), met inachtneming van de nieuwste technologie en in overeenstemming met de risico's voor de categorieën verwerkte gegevens en de kans dat overheidsinstanties proberen hier toegang toe te krijgen.***

Andere artikelen

136. ***Vaststelling en regelmatige herziening van interne beleidsmaatregelen om na te gaan in hoeverre de uitgevoerde maatregelen geschikt zijn en waar nodig extra of alternatieve oplossingen vast te stellen en uit te voeren, om te verzekeren dat er aan de doorgegeven gegevens in grote lijnen een beschermingsniveau wordt verleend dat overeenkomt met het in de EU gewaarborgde niveau.***

***

137. ***Toezeggingen van de gegevensimporteur dat hij de persoonsgegevens niet verder zal doorgeven binnen hetzelfde derde land of andere derde landen, of lopende doorgiften opschort wanneer niet kan worden gewaarborgd dat het beschermingsniveau van de persoonsgegevens in het derde land in grote lijnen overeenkomt met het binnen de EU verleende niveau.***[88]

[88] C-311/18 (Schrems II), punten 135 en 137.

BIJLAGE 3: MOGELIJKE INFORMATIEBRONNEN VOOR DE BEOORDELING VAN EEN DERDE LAND

138. Uw gegevensimporteur moet in staat zijn u te voorzien van relevante bronnen en informatie over het derde land waar hij is gevestigd en de voor hem geldende wetgeving. U kunt ook andere informatiebronnen raadplegen, zoals de bronnen die hieronder niet-uitputtend worden vermeld.

- Rechtspraak van het Hof van Justitie van de Europese Unie (HvJ-EU) en het Europees Hof voor de Rechten van de Mens (EHRM)[89] waarnaar wordt verwezen in de aanbevelingen inzake Europese essentiële garanties;[90]
- Adequaatheidsbesluiten in het land van bestemming wanneer de doorgifte op een afwijkende rechtsgrondslag is gebaseerd;[91]
- Verordeningen en verslagen van intergouvernementele organisaties zoals de Raad van Europa[92] en andere regionale organen[93] en VN-organen en agentschappen (b.v. de Raad voor de mensenrechten[94] en het mensenrechtencomité van de VN[95]);
- Nationale rechtspraak of genomen besluiten van onafhankelijke juridische of administratieve autoriteiten met bevoegdheid op het gebied van gegevensprivacy en gegevensbescherming van derde landen;
- Rapporten van wetenschappelijke instellingen en maatschappelijke organisaties (b.v. ngo's en beroepsorganisaties).

[89] Zie het informatieblad over de rechtspraak van het EHRM met betrekking tot grootschalige surveillance: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf
[90] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions
[91] C-311/18 (Schrems II), punt 141; zie de adequaatheidsbesluiten op https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[92] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions
[93] Zie bijvoorbeeld de landenrapporten van de Inter-Amerikaanse Commissie voor de mensenrechten (IACHR), https://www.oas.org/en/iachr/reports/country.asp.
[94] Zie https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx
[95] zie: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5