Aanbevelingen

Aanbevelingen 01/2021 over de adequaatheidsreferentie in het kader van de richtlijn gegevensbescherming bij rechtshandhaving

Vastgesteld op 2 februari 2021

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

Versiegeschiedenis

Versie 1.1	6 juli 2021	Wijziging in formattering
Versie 1.0	2 februari 2021	Goedkeuring van de aanbevelingen

Inhoudsopgave

Het Europees Comité voor gegevensbescherming

Gezien artikel 51, lid 1, punt b), van Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad[1],

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

HEEFT DE VOLGENDE AANBEVELINGEN VASTGESTELD

1. INLEIDING

1. De Groep gegevensbescherming artikel 29 (WP29) heeft een werkdocument[2] gepubliceerd over adequaatheidsreferentie in het kader van de algemene verordening gegevensbescherming (AVG)[3]. Het Europees Comité voor gegevensbescherming (EDPB) heeft dit werkdocument tijdens zijn eerste plenaire vergadering goedgekeurd.

2. Zoals vermeld in verklaring nr. 21 bij het Verdrag van Lissabon, kunnen specifieke regels inzake de bescherming van persoonsgegevens en het vrije verkeer van die gegevens op het gebied van justitiële samenwerking in strafzaken en politiële samenwerking op basis van artikel 16 van het Verdrag betreffende de werking van de Europese Unie (VWEU) noodzakelijk blijken vanwege de specifieke aard van deze gebieden.

3. Op basis hiervan heeft de EU-wetgever Richtlijn (EU) 2016/680 (richtlijn gegevensbescherming bij rechtshandhaving) vastgesteld, waarin specifieke regels zijn vastgelegd met betrekking tot de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op **de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaar voor de openbare veiligheid**.

4. De richtlijn gegevensbescherming bij rechtshandhaving bepaalt op welke gronden de doorgifte van persoonsgegevens aan een derde land of een internationale organisatie in dit verband is toegestaan. Een van de gronden voor een dergelijke doorgifte is het besluit van de Europese Commissie dat het betreffende derde land of de betreffende internationale organisatie een passend beschermingsniveau waarborgt.

[1] PB L 119 van 4.5.2016, blz. 89.
[2] WP254.rev01, vastgesteld door de Groep gegevensbescherming artikel 29 op 28 november 2017, laatstelijk gewijzigd en vastgesteld op 6 februari 2018. Het actualiseert hoofdstuk I van het werkdocument "Doorgifte van persoonsgegevens naar derde landen: toepassing van de artikelen 25 en 26 van de EU-richtlijn betreffende gegevensbescherming", WP12, vastgesteld door de Groep gegevensbescherming artikel 29 op 24 juli 1998.
[3] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 26 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), PB L 119 van 4.5.2016, blz. 1.

5. Waar het werkdocument WP254.rev01 over adequaatheidsreferentie tot doel heeft de Europese Commissie richtsnoeren te verstrekken over het niveau van gegevensbescherming in derde landen en bij internationale organisaties in het kader van de AVG, beoogt dit document soortgelijke richtsnoeren te verstrekken in het kader van de richtlijn gegevensbescherming bij rechtshandhaving. In dit verband worden in dit document de kernbeginselen inzake gegevensbescherming vastgesteld die in het rechtskader van een derde land of internationale organisatie aanwezig moeten zijn om ervoor te zorgen dat het beschermingsniveau in wezen overeenkomt met het EU-kader binnen het toepassingsgebied van de richtlijn gegevensbescherming bij rechtshandhaving (d.w.z. voor de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen). Daarnaast kan het als leidraad dienen voor derde landen en internationale organisaties die aan de eisen voor adequaatheid willen voldoen.

6. Dit document richt zich uitsluitend op adequaatheidsbesluiten. Dit zijn uitvoeringshandelingen van de Europese Commissie overeenkomstig artikel 36, lid 3, van de richtlijn gegevensbescherming bij rechtshandhaving.

2. HET BEGRIP ADEQUAATHEID

7. De richtlijn gegevensbescherming bij rechtshandhaving stelt de regels vast voor de doorgifte van persoonsgegevens aan derde landen en internationale organisaties, voor zover dergelijke doorgiften binnen het toepassingsgebied ervan vallen. De regels inzake internationale doorgiften van persoonsgegevens zijn vastgelegd in hoofdstuk V van de richtlijn gegevensbescherming bij rechtshandhaving, en met name in de artikelen 35 tot en met 39.

8. Overeenkomstig artikel 36 van de richtlijn gegevensbescherming bij rechtshandhaving kunnen gegevens worden doorgegeven aan een derde land of een internationale organisatie indien een derde land, een gebied of een of meerdere nader bepaalde sectoren in een derde land of een internationale organisatie een passend beschermingsniveau waarborgen. Uit de rechtspraak van het Hof van Justitie van de Europese Unie (Hof)[4] vloeit voort dat deze bepaling moet worden gelezen in het licht van artikel 35 van de richtlijn gegevensbescherming bij rechtshandhaving, met de titel “Algemeen beginsel inzake doorgifte van persoonsgegevens”, dat bepaalt dat “alle bepalingen [van hoofdstuk V van de richtlijn gegevensbescherming bij rechtshandhaving] worden toegepast opdat het door deze richtlijn gewaarborgde beschermingsniveau voor natuurlijke personen niet wordt ondermijnd”.

9. Wanneer de Europese Commissie heeft besloten dat een dergelijk passend beschermingsniveau wordt gewaarborgd, kunnen persoonsgegevens naar dat derde land, dat gebied, die sector of die internationale organisatie worden doorgegeven zonder dat daarvoor specifieke toestemming nodig is, behalve wanneer een andere lidstaat van waaruit de gegevens zijn verkregen, toestemming voor de doorgifte moet verlenen, zoals bepaald in de artikelen 35 en 36 en overweging 66 van de richtlijn gegevensbescherming bij rechtshandhaving. Dit doet geen afbreuk aan de noodzaak dat de autoriteiten van de betrokken lidstaten gegevens verwerken overeenkomstig de nationale bepalingen die ter uitvoering van Richtlijn (EU) 2016/680 zijn vastgesteld.

[4] Zaak C-311/18, Data Protection Commissioner/Facebook Ireland Ltd en Maximillian Schrems, 16 juli 2020, ECLI:EU:C:2020:559, punt 92 (Schrems II).

10. Dit begrip “passend beschermingsniveau”, dat al werd gehanteerd in Richtlijn 95/46/EG[5] en Kaderbesluit 2008/977/JBZ van de Raad[6], is in dit verband en onlangs in het kader van de AVG verder uitgewerkt door het Hof.

11. Volgens het Hof moet het beschermingsniveau in het derde land in grote lijnen overeenkomen met het niveau dat in de Unie wordt gewaarborgd, “ook al kunnen de middelen waarmee dat derde land voor waarborgen voor een passend beschermingsniveau kan zorgen, anders zijn dan die welke binnen de Unie worden ingezet”, maar “deze middelen moeten in de praktijk niettemin doeltreffend genoeg blijken te zijn”[7]. De adequaatheidsnorm vereist dus niet dat de EU-wetgeving punt voor punt wordt gekopieerd, maar dat de grote lijnen — kernvereisten — van die wetgeving worden aangehouden.

12. In dit verband heeft het Hof ook verduidelijkt dat een adequaatheidsbesluit van de Commissie een vaststelling moet bevatten ten aanzien van de vraag of er, in het derde land, door dat land vastgestelde regels bestaan ter beperking van inmengingen in de grondrechten van de personen van wie de gegevens vanuit de Europese Unie naar dat derde land worden doorgegeven, waarbij geldt dat de overheidsinstanties van dat land tot een dergelijke inmenging *mogen* overgaan wanneer zij legitieme doelstellingen, zoals nationale veiligheid, nastreven[8].

13. Het doel van adequaatheidsbesluiten van de Europese Commissie is formeel te bevestigen, met bindende gevolgen voor de lidstaten[9], met inbegrip van hun bevoegde gegevensbeschermingsautoriteiten[10], dat het niveau van gegevensbescherming in een derde land of bij een internationale organisatie in grote lijnen overeenkomt met het niveau van gegevensbescherming in de Europese Unie. Het derde land dient waarborgen te bieden voor een adequaat beschermingsniveau dat in wezen overeenkomt met het beschermingsniveau in de Unie, vooral wanneer gegevens in een of meerdere nader bepaalde sectoren worden verwerkt[11].

14. Adequaatheid kan worden bereikt door een combinatie van rechten voor de betrokkenen, verplichtingen voor gegevensverwerkers of verwerkingsverantwoordelijken en toezicht door onafhankelijke instanties. Regelgeving voor gegevensverwerking is echter alleen doeltreffend als zij afdwingbaar is en in de praktijk wordt nageleefd. Daarom moet niet alleen worden gekeken naar de inhoud van de regels die van toepassing zijn op persoonsgegevens die naar een derde land of een internationale organisatie worden doorgegeven, maar ook naar het bestaande systeem om de doeltreffendheid van dergelijke regels te waarborgen. Voor de doeltreffendheid van gegevensbeschermingsregels zijn efficiënte handhavingsmechanismen van doorslaggevend belang[12].

---

[5] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, PB L 281 van 23.11.1995, blz. 31.

[6] Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, PB L 350 van 30.12.2008, blz. 60.

[7] Zaak C-362/14, Maximillian Schrems/Data Protection Commissioner, 6 oktober 2015, ECLI:EU:C:2015:650, punten 73 en 74 (Schrems I).

[8] Schrems I, punt 88.

[9] Artikel 288 VWEU.

[10] Schrems I, punt 52.

[11] Overweging 67, richtlijn gegevensbescherming bij rechtshandhaving.

[12] Schrems I, punten 72-74, en advies 1/15 van het Hof over het ontwerp van overeenkomst tussen Canada en de Europese Unie, 26 juli 2017, ECLI:EU:C:2017:592 (Advies 1/15), punt 134: “Dit recht op bescherming van persoonsgegevens vereist met name dat het door het Unierecht gewaarborgde hoge beschermingsniveau van de

3. PROCEDURELE ASPECTEN VAN ADEQUAATHEIDSBEVINDINGEN IN HET KADER VAN DE RICHTLIJN GEGEVENSBESCHERMING BIJ RECHTSHANDHAVING

15. Om de Europese Commissie overeenkomstig artikel 51, lid 1, punt g), van de richtlijn gegevensbescherming bij rechtshandhaving te adviseren, moet de EDPB alle relevante documentatie ontvangen, met inbegrip van relevante correspondentie en de bevindingen van de Europese Commissie. Het is absoluut noodzakelijk dat alle relevante documenten lang genoeg van tevoren aan de EDPB worden toegezonden en in het Engels worden vertaald om een geïnformeerde en nuttige discussie mogelijk te maken voordat adequaatheidsbesluiten definitief worden vastgesteld. In het geval van een complex rechtskader gaat het daarbij ook om eventuele rapporten over het gegevensbeschermingsniveau in het derde land of de internationale organisatie. In ieder geval moet de door de Europese Commissie verstrekte informatie uitputtend zijn en de EDPB in staat stellen de door de Commissie uitgevoerde analyse van het gegevensbeschermingsniveau in het derde land of de internationale organisatie te beoordelen.

16. De EDPB verstrekt te gelegener tijd een advies over de bevindingen van de Europese Commissie, stelt eventuele tekortkomingen in het adequaatheidskader vast en doet waar nodig mogelijke aanbevelingen.

17. Overeenkomstig artikel 36, lid 4, van de richtlijn gegevensbescherming bij rechtshandhaving is het aan de Europese Commissie om — op permanente basis — toe te zien op ontwikkelingen die van invloed kunnen zijn op de werking van een adequaatheidsbesluit.

18. Artikel 36, lid 3, van de richtlijn gegevensbescherming bij rechtshandhaving bepaalt dat ten minste om de vier jaar een periodieke toetsing moet plaatsvinden. Dit is echter een algemeen tijdsbestek dat moet worden aangepast aan elk derde land of elke internationale organisatie waarvoor een adequaatheidsbesluit is genomen. Afhankelijk van de specifieke omstandigheden kan een kortere evaluatiecyclus nodig zijn. Ook incidenten of nieuwe informatie over of wijzigingen in het rechtskader van het derde land of de internationale organisatie in kwestie kunnen aanleiding vormen om de toetsing eerder dan gepland uit te voeren. Het is waarschijnlijk een passende werkwijze de eerste toetsing van een volkomen nieuw adequaatheidsbesluit vrij snel uit te voeren en geleidelijk de evaluatiecyclus aan te passen al naargelang de resultaten.

19. Gezien zijn taak om aan de Europese Commissie een advies te verstrekken over de vraag of het derde land, een gebied of een of meerdere nader bepaalde sectoren in dit derde land of een internationale organisatie nog wel een passend beschermingsniveau waarborgt, moet de EDPB tijdig zinvolle informatie ontvangen over het toezicht door de Europese Commissie op de relevante ontwikkelingen in dat derde land of die internationale organisatie door de Europese Commissie. Daarom moet de EDPB op de hoogte worden gehouden van alle evaluatieprocessen en -missies in het derde land of bij de internationale organisatie. De EDPB beveelt aan te worden uitgenodigd om deel te nemen aan deze evaluatieprocessen en -missies, zoals voorzien in het privacyschildbesluit en opgenomen in het adequaatheidsbesluit met betrekking tot Japan.

---

vrijheden en grondrechten behouden blijft ingeval persoonsgegevens van de Unie naar een derde land worden doorgegeven. De middelen waarmee dit beschermingsniveau wordt gewaarborgd, mogen weliswaar verschillen van die welke binnen de Unie worden ingezet om voor naleving van de uit het Unierecht voortvloeiende vereisten te zorgen, maar deze middelen moeten in de praktijk wel doeltreffend genoeg blijken om een bescherming te bieden die in grote lijnen overeenkomt met die welke binnen de Unie wordt gewaarborgd."

20. Verder moet worden opgemerkt dat de Europese Commissie overeenkomstig artikel 36, lid 5, van de richtlijn gegevensbescherming bij rechtshandhaving bevoegd is om, wanneer het derde land of de internationale organisatie niet langer een passend beschermingsniveau waarborgt, bestaande adequaatheidsbesluiten in te trekken, te wijzigen of op te schorten. Bij de procedure om het besluit in te trekken, te wijzigen of op te schorten, wordt de EDPB gevraagd advies uit te brengen, overeenkomstig artikel 51, lid 1, punt g), van de richtlijn gegevensbescherming bij rechtshandhaving.

21. Onverminderd de bevoegdheden van de met vervolging belaste autoriteiten moeten toezichthoudende autoriteiten bovendien de bevoegdheid hebben inbreuken op deze richtlijn onder de aandacht van de gerechtelijke autoriteiten te brengen of in rechte op te treden[13]. Uit het arrest-Schrems I van het Hof vloeit met name voort dat gegevensbeschermingsautoriteiten in rechte moeten kunnen optreden bij de nationale rechter indien zij een vordering van een persoon tegen een adequaatheidsbesluit gegrond achten[14]. Het arrest-Schrems II bevestigde deze beoordeling[15].

4. EU-NORMEN VOOR ADEQUAATHEID BIJ POLITIËLE SAMENWERKING EN JUSTITIËLE SAMENWERKING IN STRAFZAKEN

22. Inhoudelijk moeten adequaatheidsbesluiten gericht zijn op de beoordeling van de bestaande wetgeving van het derde land als geheel, in theorie en in de praktijk, in het licht van de beoordelingscriteria van artikel 36 van de richtlijn gegevensbescherming bij rechtshandhaving. Het systeem van een derde land of een internationale organisatie moet de volgende algemene, procedurele en handhavingsbeginselen en -mechanismen inzake gegevensbescherming bevatten.

23. In artikel 36, lid 2, van de richtlijn gegevensbescherming bij rechtshandhaving worden de elementen vastgesteld waarmee de Europese Commissie rekening moet houden bij de beoordeling van de adequaatheid van het beschermingsniveau in een derde land of een internationale organisatie.

24. De Commissie houdt met name rekening met de rechtsstatelijkheid, de eerbiediging van de mensenrechten en de fundamentele vrijheden[16], relevante wetgeving, alsook met de uitvoering

[13] Zie artikel 47, lid 5, van de richtlijn gegevensbescherming bij rechtshandhaving en overweging 82 daarvan.
[14] Zie Schrems I, punt 65: "In dat verband staat het aan de nationale wetgever om in beroepsgangen te voorzien waarmee bedoelde autoriteit de grieven die zij gegrond acht aan de nationale rechter kan voorleggen, zodat die laatste, wanneer hij de twijfel ten aanzien van de geldigheid van de beschikking van de Commissie deelt, de vraag naar de geldigheid van die beschikking prejudicieel kan verwijzen."
[15] Zie Schrems II, punt 120: "Zelfs indien de Commissie een adequaatheidsbesluit heeft vastgesteld, moet de bevoegde nationale toezichthoudende autoriteit waarbij een persoon een klacht heeft ingediend met betrekking tot de bescherming van zijn rechten en vrijheden in verband met een verwerking van hem betreffende persoonsgegevens, dus in volledige onafhankelijkheid kunnen onderzoeken of de doorgifte van die gegevens voldoet aan de vereisten van de AVG en, in voorkomend geval, beroep kunnen instellen bij de nationale rechterlijke instanties, opdat laatstbedoelde instanties, indien zij de twijfels van die autoriteit over de geldigheid van het besluit delen, de vraag naar die geldigheid prejudicieel kunnen verwijzen."
[16] Bij de beoordeling van het rechtskader van het derde land moet rekening worden gehouden met de mogelijkheid dat de doodstraf of enige vorm van wrede en onmenselijke behandeling kan worden opgelegd op basis van gegevens die vanuit de EU worden doorgegeven. Indien de wetgeving van het derde land in een dergelijke straf of behandeling voorziet, moeten in het rechtskader van het derde land aanvullende waarborgen worden gevonden

van die wetgeving, doeltreffende en afdwingbare rechten van betrokkenen en doeltreffende administratieve en gerechtelijke beroepsmogelijkheden voor de betrokkenen wier persoonsgegevens worden doorgegeven, het bestaan en het effectief functioneren van een of meer onafhankelijke toezichthoudende autoriteiten en de internationale verplichtingen die het derde land of de internationale organisatie heeft aangegaan.

25. Het is dan ook duidelijk dat een zinvolle analyse van passende bescherming twee basiselementen moet bevatten: de inhoud van de toepasselijke regels en de middelen om de doeltreffende toepassing ervan in de praktijk te waarborgen. Het is de taak van de Europese Commissie om — periodiek — na te gaan of de geldende regels in de praktijk doeltreffend zijn.

26. De inhoudelijke kernbeginselen voor gegevensbescherming en de eisen ten aanzien van procedures en handhaving, die kunnen worden beschouwd als een minimumvereiste voor adequate bescherming, zijn afgeleid van het Handvest van de grondrechten van de Europese Unie (hierna "het Handvest") en de richtlijn gegevensbescherming bij rechtshandhaving. Algemene bepalingen inzake gegevensbescherming en bescherming van de persoonlijke levenssfeer in het derde land volstaan niet. In het rechtskader van het derde land of de internationale organisatie moeten daarentegen specifieke bepalingen worden opgenomen die concreet betrekking hebben op het recht op gegevensbescherming bij rechtshandhaving. Het derde land moet waarborgen bieden voor een passend beschermingsniveau dat in wezen overeenkomt met het niveau dat binnen de Unie wordt gewaarborgd. De naleving van deze bepalingen moet afdwingbaar zijn.

27. Wat voorts het evenredigheidsbeginsel betreft[17], heeft het Hof met betrekking tot de wetgeving van de lidstaten geoordeeld dat bij de beoordeling of een beperking van het recht op bescherming van de persoonlijke levenssfeer en het recht op gegevensbescherming gerechtvaardigd kan zijn, enerzijds moet worden bepaald wat de **ernst is van de inmenging** die een dergelijke beperking meebrengt[18], en anderzijds moet worden nagegaan of het **belang van de doelstelling van algemeen belang** dat met die beperking wordt nagestreefd, in verhouding staat tot die ernst[19].

28. Volgens de rechtspraak van het Hof moet een wettelijke grondslag op grond waarvan inmenging in de grondrechten mogelijk is, om te voldoen aan het evenredigheidsbeginsel, zelf de omvang van de beperking van de uitoefening van het betrokken recht bepalen[20]. Uitzonderingen op en beperkingen van de bescherming van persoonsgegevens mogen slechts gelden voor zover dat strikt noodzakelijk is[21]. Om aan dit vereiste te voldoen, moet de betrokken wetgeving niet alleen duidelijke en precieze regels voor de reikwijdte en de toepassing van de betrokken maatregel bevatten, maar ook minimale eisen opleggen, zodat de personen van wie de gegevens zijn doorgegeven, over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik. "Zij moet in het bijzonder aangeven in welke

om ervoor te zorgen dat uit de EU doorgegeven gegevens niet worden gebruikt om een doodstraf of enige vorm van wrede of onmenselijke behandeling te vragen, uit te spreken of uit te voeren (bv. een internationale overeenkomst die voorwaarden oplegt aan de doorgifte, een toezegging van het derde land om geen doodstraf of enige vorm van wrede en onmenselijke behandeling op te leggen op basis van uit de EU doorgegeven gegevens of een moratorium op de doodstraf).

[17] Artikel 52, lid 1, van het Handvest.

[18] De rechter merkte bijvoorbeeld op dat "de inmenging die de opvraging in real time van gegevens aan de hand waarvan een eindapparaat kan worden gelokaliseerd, met zich brengt, bijzonder ernstig is, aangezien die gegevens de bevoegde nationale autoriteiten in staat stellen om de verplaatsingen van gebruikers van mobiele telefoons nauwkeurig en permanent te volgen [...]" (gevoegde zaken C-511/18, C-512/18 en C-520/18, La Quadrature du Net e.a., 6 oktober 2020, ECLI:EU:C:2020:791, punt 187 en aldaar aangehaalde rechtspraak).

[19] La Quadrature du Net e.a., punt 131.

[20] Schrems II, punt 180.

[21] Schrems II, punt 176 en aldaar aangehaalde rechtspraak.

omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens automatisch worden verwerkt"[22].

29. De EDPB heeft aanbevelingen vastgesteld met essentiële garanties die in overeenstemming zijn met de rechtspraak van het Hof en het Europees Hof voor de Rechten van de Mens (EHRM) op het gebied van surveillance die in het recht van het derde land kunnen worden aangetroffen bij de beoordeling van de inmenging van dergelijke surveillancemaatregelen van derde landen in de rechten van betrokkenen ingeval de gegevens overeenkomstig de AVG aan dat derde land worden doorgegeven[23]. Om te beoordelen of aan de voorwaarden van artikel 36, lid 2, punt a), van de richtlijn gegevensbescherming bij rechtshandhaving is voldaan, is de EDPB van mening dat bij de beoordeling van de adequaatheid van een derde land in het kader van de richtlijn gegevensbescherming bij rechtshandhaving op het gebied van surveillance rekening moet worden gehouden met de in deze aanbevelingen vervatte garanties, rekening houdend met verdere specifieke voorwaarden op het gebied van surveillance in dit verband.

30. Met betrekking tot artikel 36, lid 2, punt b), moet het derde land niet alleen zorgen voor doeltreffend onafhankelijk gegevensbeschermingstoezicht, maar ook voor mechanismen voor samenwerking met de gegevensbeschermingsautoriteiten van de lidstaten[24].

31. Met betrekking tot artikel 36, lid 2, punt c), moet, afgezien van de internationale verplichtingen die het derde land of de internationale organisatie heeft aangegaan, ook rekening worden gehouden met de verplichtingen die voortvloeien uit de deelname van het derde land of de internationale organisatie aan multilaterale of regionale regelingen, in het bijzonder wat de bescherming van persoonsgegevens betreft, alsook met de nakoming van die verplichtingen, met name de toetreding van het derde land tot andere internationale overeenkomsten inzake gegevensbescherming, bijvoorbeeld het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens en het bijbehorende Aanvullend Protocol (Verdrag 108[25] en de gemoderniseerde versie, Verdrag 108+). Er kan ook rekening worden gehouden met de naleving door het derde land van beginselen die zijn vastgelegd in internationale documenten, zoals de "Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime may also be taken into account".

32. Een adequaatheidsbesluit moet ervoor zorgen dat het buitenlandse systeem als geheel, door de inhoud van de rechten op het gebied van bescherming van de persoonlijke levenssfeer en gegevensbescherming en de doeltreffende uitvoering, toezicht en handhaving daarvan, het vereiste beschermingsniveau biedt, ook voor gegevens in doorvoer naar dit derde land. Zoals het Hof in het arrest-Schrems II heeft benadrukt, moet het hoge niveau van bescherming ook worden gewaarborgd bij doorgifte van gegevens naar een derde land[26].

33. Tot slot moet de Europese Commissie bij de vaststelling van een adequaatheidsbesluit met betrekking tot een gebied of een nader bepaalde sector in een derde land rekening houden met

[22] Schrems II, punt 176 en aldaar aangehaalde rechtspraak.
[23] EDPB-aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, vastgesteld op 10 november 2020.
[24] Overweging 67, richtlijn gegevensbescherming bij rechtshandhaving.
[25] Overweging 68, richtlijn gegevensbescherming bij rechtshandhaving.
[26] Zie punt 93.

duidelijke en objectieve criteria, zoals specifieke verwerkingsactiviteiten of het toepassingsgebied van de toepasselijke wettelijke normen en geldende wetgeving in het derde land[27].

A. Algemene beginselen en waarborgen

a) Begrippen

34. Er moeten basisbegrippen voor gegevensbescherming bestaan. Deze hoeven geen kopie te zijn van de terminologie die in de richtlijn gegevensbescherming bij rechtshandhaving wordt gehanteerd, maar moeten wel een afspiegeling vormen van de begrippen in de Europese wetgeving inzake gegevensbescherming en daarmee consistent zijn. In de richtlijn gegevensbescherming bij rechtshandhaving zijn bijvoorbeeld de volgende belangrijke begrippen opgenomen: "persoonsgegevens", "verwerking van persoonsgegevens", "bevoegde autoriteiten", "verwerkingsverantwoordelijke", "verwerker", "ontvanger", "gevoelige gegevens", "nauwkeurigheid", "profilering", "gegevensbescherming door ontwerp en door standaardinstellingen", "toezichthoudende autoriteit" en "pseudonimisering".

b) Rechtmatigheid en behoorlijkheid van de verwerking van persoonsgegevens (artikel 4 — overweging 26)

35. Volgens artikel 8, lid 2, van het Handvest moeten persoonsgegevens onder meer worden verwerkt "voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet"[28]. In het kader van rechtshandhaving moet echter worden opgemerkt dat de uitvoering van de bij wet aan de bevoegde autoriteiten opgedragen taken op het gebied van het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten het hun mogelijk maakt natuurlijke personen te verplichten of te gelasten gevolg te geven aan de ingediende verzoeken. In dat geval mag de toestemming van de betrokkene geen rechtsgrond vormen voor de verwerking van persoonsgegevens door bevoegde autoriteiten[29].

36. Deze wettelijke grondslag moet duidelijke en nauwkeurige regels bevatten die de reikwijdte en de toepassing van de betrokken verwerkingsactiviteiten bepalen en minimale eisen opleggen[30]. Daarnaast herinnerde het Hof eraan dat een "regeling [...] wettelijk verbindend [moet] zijn naar intern recht"[31].

37. Om rechtmatig te zijn, moet de gegevensverwerking[32] noodzakelijk zijn voor de uitvoering van een taak door een bevoegde autoriteit met het oog op de voorkoming, het onderzoek, de

[27] Overweging 67, richtlijn gegevensbescherming bij rechtshandhaving.
[28] Zie Schrems II, punt 173.
[29] In overweging 35 van de richtlijn gegevensbescherming bij rechtshandhaving staat ook dat "[w]anneer van de betrokkene wordt verlangd dat hij aan een wettelijke verplichting voldoet, [...] hij geen echte, vrije keuze [heeft], en [...] zijn reactie derhalve niet als een spontane blijk van zijn wil [kan] worden uitgelegd. Dit mag de lidstaten niet beletten om in hun wetgeving te bepalen dat de betrokkene kan instemmen met de verwerking van zijn persoonsgegevens voor de doeleinden van deze richtlijn, zoals DNA-tests in strafrechtelijke onderzoeken of het toezicht, met behulp van elektronische enkelbanden, op de locatie waar de betrokkene zich bevindt met het oog op de tenuitvoerlegging van straffen."
[30] Zie Schrems II, punten 175 en 180, en advies 1/15, punt 139 en aldaar aangehaalde rechtspraak.
[31] Zie zaak C-623/17, Privacy International/Secretary of State for Foreign and Commonwealth Affairs e.a., 6 oktober 2020, ECLI:EU:C:2020:790, punt 68 — Het moet ook duidelijk zijn dat het Hof in de Franse versie van het arrest het woord "*réglementation*" gebruikt dat ruimer is dan alleen handelingen van het Parlement.
[32] De geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens en de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaar voor de openbare veiligheid[33]. Deze doeleinden moeten in het interne recht zijn vastgelegd.

38. Persoonsgegevens worden behoorlijk verwerkt. Het gegevensbeschermingsbeginsel van behoorlijke verwerking is een ander begrip dan het recht op een onpartijdig gerecht zoals omschreven in artikel 47 van het Handvest en artikel 6 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM)[34].

c) Het beginsel van doelbinding (artikel 4)

39. De specifieke doeleinden waarvoor de persoonsgegevens worden verwerkt, moeten expliciet en legitiem zijn en worden vastgesteld op het ogenblik dat de persoonsgegevens worden verzameld[35].

40. De gegevens moeten worden verwerkt voor een specifiek, uitdrukkelijk en legitiem doel met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen[36], met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid in het derde land, en vervolgens worden gebruikt voor een van deze doeleinden, voor zover dit niet onverenigbaar is met het oorspronkelijke doel van de verwerking (bv. voor parallelle tenuitvoerleggingsprocedures of archivering in het algemeen belang, wetenschappelijk, statistisch of historisch gebruik voor dergelijke doeleinden) en met inachtneming van passende waarborgen voor de rechten en vrijheden van de betrokkenen. Indien persoonsgegevens worden verwerkt door dezelfde of een andere verwerkingsverantwoordelijke (bevoegde autoriteit[37]) met het oog op het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten of het ten uitvoer leggen van straffen, wat niet de doelstelling is waarvoor zij zijn verzameld, moet deze verwerking worden toegestaan, op voorwaarde dat zij is toegestaan op grond van toepasselijke wettelijke bepalingen, noodzakelijk is en in verhouding staat tot die andere doelstelling[38]. Er moet ook rekening worden gehouden met het bestaan van een mechanisme om de bevoegde autoriteiten van de betrokken lidstaten in kennis te stellen van een dergelijke verdere verwerking van gegevens[39]. Bovendien mag het in de Unie door de richtlijn gegevensbescherming bij rechtshandhaving geboden beschermingsniveau van natuurlijke personen in geen geval worden ondermijnd, ook niet wanneer persoonsgegevens vanuit het

[33] Bevoegde autoriteiten zijn elke overheidsinstantie die daartoe bevoegd is of ieder ander orgaan dat of iedere andere entiteit die bij wet is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen voor dergelijke doeleinden.
[34] Overweging 26, richtlijn gegevensbescherming bij rechtshandhaving.
[35] Overweging 26, richtlijn gegevensbescherming bij rechtshandhaving.
[36] Hieronder vallen ook "politieactiviteiten waarbij vooraf niet bekend is of een voorval al dan niet een strafbaar feit is. Tot die activiteiten behoren ook de uitoefening van gezag door het nemen van dwangmaatregelen zoals politieactiviteiten bij demonstraties, belangrijke sportevenementen en rellen. Zij omvatten ook de rechts- en ordehandhaving als een, zo nodig, aan de politie of andere rechtshandhavingsautoriteiten toevertrouwde taak ter bescherming tegen en voorkoming van gevaren voor de openbare veiligheid en voor bij wet beschermde fundamentele belangen van de samenleving, die tot strafbare feiten kunnen leiden" (overweging 12, richtlijn gegevensbescherming bij rechtshandhaving). Het moet worden onderscheiden van een doel van nationale veiligheid of activiteiten die binnen het toepassingsgebied van titel V, hoofdstuk 2, van het Verdrag betreffende de Europese Unie (VEU) vallen (overweging 14, richtlijn gegevensbescherming bij rechtshandhaving).
[37] Zie voetnoot 33.
[38] Overweging 29, richtlijn gegevensbescherming bij rechtshandhaving.
[39] Een dergelijk mechanisme kan bijvoorbeeld bestaan uit onderling overeengekomen verwerkingscodes, een kennisgevingsverplichting uit hoofde van een internationaal instrument, met inbegrip van mogelijke geautomatiseerde kennisgevingen, of andere soortgelijke transparantiemaatregelen.

derde land worden doorgegeven aan verwerkingsverantwoordelijken of verwerkers in hetzelfde derde land[40].

d) Specifieke voorwaarden voor verdere verwerking voor andere doeleinden (artikel 9)

41. De verdere verwerking of openbaarmaking van gegevens die vanuit de EU worden doorgegeven voor andere doeleinden dan rechtshandhaving, zoals nationale veiligheidsdoeleinden, moet ook bij wet worden geregeld, noodzakelijk en evenredig zijn. Er moet ook rekening worden gehouden met het bestaan van een mechanisme om de bevoegde autoriteiten van de betrokken lidstaten in kennis te stellen van een dergelijke verdere verwerking van gegevens[41]. Ook hier moeten de gegevens na verdere verwerking of openbaarmaking hetzelfde beschermingsniveau genieten als wanneer zij oorspronkelijk door de ontvangende bevoegde autoriteit werden verwerkt.

e) Het beginsel van gegevensminimalisatie

42. De gegevens moeten toereikend, ter zake dienend en niet bovenmatig zijn in verhouding tot de doeleinden waarvoor zij worden verwerkt. Met name moet rekening worden gehouden met de toepassing van de voorschriften inzake gegevensbescherming door ontwerp en standaardinstellingen, zoals beperkte invoervelden (gestructureerde communicatie) of geautomatiseerde en niet-geautomatiseerde kwaliteitscontroles.

f) Het beginsel van juistheid van gegevens

43. De gegevens moeten juist zijn en zo nodig worden bijgewerkt. Niettemin moet bij de toepassing van het beginsel van juistheid van de gegevens rekening worden gehouden met de aard en het doel van de betrokken verwerking. In het bijzonder bij gerechtelijke procedures zijn verklaringen die persoonsgegevens bevatten, gebaseerd op de subjectieve perceptie van natuurlijke personen en niet altijd te controleren. Het vereiste van juistheid dient derhalve geen betrekking te hebben op de juistheid van een verklaring, maar alleen op het feit dat een specifieke verklaring is afgelegd[42].

44. Er moet voor worden gezorgd dat persoonsgegevens die onjuist, onvolledig of niet langer actueel zijn, niet worden doorgegeven of ter beschikking worden gesteld[43] en dat procedures worden ingesteld om onjuiste gegevens te corrigeren of te verwijderen. Er moet met name rekening worden gehouden met elk classificatiesysteem van de verwerkte informatie, wat de betrouwbaarheid van de bron en het niveau van verificatie van de feiten betreft[44].

g) Het beginsel van gegevensbewaring

45. De gegevens mogen niet langer worden bewaard dan nodig is voor de doeleinden waarvoor zij worden verwerkt. Er moeten passende mechanismen worden vastgesteld voor het wissen van persoonsgegevens; het kan gaan om een vaste termijn of om een periodieke evaluatie van de noodzaak van de opslag van persoonsgegevens (of een combinatie van beide: een vaste maximumtermijn en periodieke evaluatie met bepaalde tussenpozen)[45]. Persoonsgegevens die

[40] Overweging 64, richtlijn gegevensbescherming bij rechtshandhaving.
[41] Zie voetnoot 39.
[42] Overweging 30, richtlijn gegevensbescherming bij rechtshandhaving.
[43] Overweging 32, richtlijn gegevensbescherming bij rechtshandhaving.
[44] Bv. 4x4-tabellen voor betrouwbaarheidsbeoordelingen en verwerkingscodes.
[45] Artikel 5, richtlijn gegevensbescherming bij rechtshandhaving.

langer worden bewaard met het oog op archivering in het algemeen belang of wetenschappelijk, statistisch of historisch gebruik, moeten worden onderworpen aan passende waarborgen (bv. met betrekking tot toegang)[46].

h) Het beginsel van beveiliging en vertrouwelijkheid (artikel 29, overwegingen 28 en 71)

46. Elke entiteit die persoonsgegevens verwerkt, moet ervoor zorgen dat de gegevens worden verwerkt op een wijze die de beveiliging van de persoonsgegevens waarborgt, onder meer door ongeoorloofde toegang tot of gebruik van persoonsgegevens en de voor de verwerking gebruikte apparatuur te voorkomen. Dit omvat bescherming tegen onrechtmatige verwerking, alsmede onopzettelijk verlies, vernietiging of beschadiging, en passende maatregelen om deze aan te pakken, met gebruikmaking van passende technische en organisatorische maatregelen. Bij het bepalen van het beveiligingsniveau moet rekening worden gehouden met de stand van de techniek, de uitvoeringskosten en de aard, reikwijdte, context en doeleinden van de verwerking, alsook met het risico van wisselende waarschijnlijkheid en ernst voor de rechten en vrijheden van natuurlijke personen.

47. Er moet worden gezorgd voor veilige communicatiekanalen tussen de autoriteiten van de lidstaten die persoonsgegevens doorgeven en de ontvangende autoriteiten van derde landen.

i) Het transparantiebeginsel (artikel 13, overwegingen 26, 39, 42, 43, 44 en 46)

48. Natuurlijke personen moeten bewust worden gemaakt van de risico's, regels, waarborgen en rechten in verband met de verwerking van hun persoonsgegevens, alsook van de wijze waarop zij hun rechten met betrekking tot de verwerking ervan kunnen uitoefenen[47].

49. Informatie over alle belangrijke elementen van de verwerking van hun persoonsgegevens moet ter beschikking van de betrokkenen worden gesteld. Deze informatie moet gemakkelijk toegankelijk en gemakkelijk te begrijpen zijn, in duidelijke en eenvoudige taal. Deze informatie moet het doel van de verwerking omvatten, de identiteit van de verwerkingsverantwoordelijke, de rechten die de betrokkene ter beschikking staan[48] en andere informatie, voor zover noodzakelijk om een behoorlijke verwerking te waarborgen.

50. Er kunnen uitzonderingen op dit informatierecht worden gemaakt. Een dergelijke beperking moet echter door middel van een wettelijke maatregel worden toegestaan en noodzakelijk en evenredig zijn om belemmering van officiële of gerechtelijke onderzoeken of procedures te voorkomen, nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen te voorkomen, de openbare veiligheid of de nationale veiligheid te beschermen, de rechten en vrijheden van anderen te beschermen, voor zover en zolang een dergelijke gedeeltelijke of volledige beperking in een democratische samenleving, met inachtneming van de grondrechten en de legitieme belangen van de natuurlijke persoon in kwestie, een noodzakelijke en evenredige maatregel is. Dergelijke beperkingen moeten ook worden overwogen en beoordeeld, rekening houdend met de mogelijkheid om een klacht in te dienen bij een toezichthoudende autoriteit of om een rechtsmiddel in te stellen. In elk geval moet elke mogelijke beperking tijdelijk en niet algemeen zijn en moet zij worden beheerst door soortgelijke voorwaarden, waarborgen en beperkingen als die welke vereist zijn krachtens het Handvest en het EVRM, zoals uitgelegd in respectievelijk de

[46] Overweging 26, richtlijn gegevensbescherming bij rechtshandhaving.
[47] Overweging 26, richtlijn gegevensbescherming bij rechtshandhaving.
[48] Zowel de materiële rechten (recht op toegang, rectificatie enz.) als het recht op verhaal.

rechtspraak van het Hof en het EHRM, en met name de wezenlijke inhoud van die rechten en vrijheden moet eerbiedigen.

j) Het recht op inzage, rectificatie en wissing van gegevens (artikelen 14 en 16)

51. De betrokkene heeft het recht uitsluitsel te krijgen over de vraag of hem of haar betreffende gegevens al dan niet worden verwerkt en, indien dat het geval is, toegang te hebben tot zijn of haar gegevens. Dit recht moet ten minste bepaalde informatie over de verwerking omvatten, zoals het doel en de rechtsgrondslag van de verwerking, het recht om een klacht in te dienen bij de toezichthoudende autoriteit of de betrokken categorieën persoonsgegevens[49]. Dit is met name van belang wanneer transparantie wordt bereikt door middel van een algemene kennisgeving (bv. informatie op de website van de autoriteit).

52. De betrokkene heeft recht op rectificatie van zijn of haar gegevens om specifieke redenen, bijvoorbeeld wanneer deze onjuist of onvolledig blijken te zijn. Ook heeft de betrokkene recht op wissing van zijn/haar persoonsgegevens wanneer de verwerking ervan bijvoorbeeld onrechtmatig of niet langer noodzakelijk is.

53. De uitoefening van die rechten mag voor de betrokkene niet buitensporig omslachtig zijn.

k) Beperkingen van de rechten van betrokkenen

54. Er kunnen mogelijke beperkingen van deze rechten bestaan om belemmering van officiële of gerechtelijke onderzoeken of procedures te voorkomen, om ervoor te zorgen dat de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen niet in het gedrang komt, om de openbare veiligheid of de nationale veiligheid te beschermen, of om de rechten en vrijheden van anderen te beschermen, voor zover en zolang een dergelijke gedeeltelijke of volledige beperking in een democratische samenleving een noodzakelijke en evenredige maatregel is, met inachtneming van de grondrechten en legitieme belangen van de betrokken natuurlijke persoon. Dergelijke beperkingen moeten ook worden overwogen en beoordeeld, rekening houdend met de mogelijkheid om een klacht in te dienen bij een toezichthoudende autoriteit of om een rechtsmiddel in te zetten.

l) Beperking van verdere doorgiften (artikel 35, overwegingen 64 en 65)

55. De verdere doorgifte van persoonsgegevens door de eerste ontvanger naar een ander derde land of een andere internationale organisatie mag geen afbreuk doen aan het in de Unie geboden beschermingsniveau van natuurlijke personen van wie gegevens worden doorgegeven. Een dergelijke verdere doorgifte van gegevens mag daarom alleen worden toegestaan indien de continuïteit van het door het EU-recht geboden beschermingsniveau is gewaarborgd[50]. In het bijzonder moet de latere ontvanger (d.w.z. de ontvanger van de verdere doorgifte) een voor rechtshandhavingsdoeleinden bevoegde autoriteit[51] zijn en mogen dergelijke verdere doorgiften van gegevens alleen plaatsvinden voor beperkte en welbepaalde doeleinden en voor zover er een rechtsgrondslag voor de verwerking is.

56. Er moet ook rekening worden gehouden met het bestaan van een mechanisme waarmee de bevoegde autoriteiten van de betrokken lidstaat in kennis worden gesteld en toestemming kunnen geven voor de verdere doorgifte van gegevens. De eerste ontvanger van de uit de EU

[49] Artikel 14, richtlijn gegevensbescherming bij rechtshandhaving.
[50] Zie ook advies 1/15.
[51] Zie voetnoot 33.

doorgegeven gegevens moet aansprakelijk zijn en moet kunnen aantonen dat de relevante bevoegde autoriteit van de lidstaat toestemming heeft gegeven voor de verdere doorgifte[52] en dat passende waarborgen worden geboden voor verdere doorgifte van gegevens indien er geen adequaatheidsbesluit is met betrekking tot het derde land waarnaar de gegevens verder zouden worden doorgegeven[53].

m) Beginsel van verantwoordingsplicht (artikel 4, lid 4)

57. De verwerkingsverantwoordelijke moet verantwoordelijk zijn voor en kunnen aantonen dat hij voldoet aan de gegevensbeschermingsbeginselen van artikel 4 van de richtlijn gegevensbescherming bij rechtshandhaving.

[52] In dit verband moet rekening worden gehouden met het bestaan van een verplichting of een verbintenis om relevante, door de autoriteiten van de overdragende lidstaten vastgestelde verwerkingscodes toe te passen.
[53] Bovenstaande vereisten laten de specifieke voorwaarden voor verdere doorgifte naar een adequaat land in het kader van de richtlijn gegevensbescherming bij rechtshandhaving onverlet (artikel 35, lid 1, punten c) en e)).

B. Voorbeelden van aanvullende beginselen die moeten worden toegepast op specifieke soorten verwerking

a) Bijzondere gegevenscategorieën (artikel 10 en overweging 37)

58. Wanneer sprake is van "bijzondere gegevenscategorieën" zijn specifieke waarborgen nodig[54], om de specifieke risico's aan te pakken[55]. Deze categorieën moeten een afspiegeling zijn van de categorieën die worden genoemd in artikel 10 van de richtlijn gegevensbescherming bij rechtshandhaving. De verwerking van bijzondere gegevenscategorieën moet daarom worden onderworpen aan specifieke waarborgen en alleen worden toegestaan wanneer dat strikt noodzakelijk is onder bepaalde voorwaarden, bijvoorbeeld om het vitale belang van een individu te beschermen.

b) Geautomatiseerde besluitvorming en profilering (artikel 11 en overweging 38)

59. Besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking (geautomatiseerde individuele besluitvorming), waaronder profilering, waaraan voor de betrokkene nadelige rechtsgevolgen zijn verbonden of die hem/haar anderszins in aanmerkelijke mate treffen, mogen uitsluitend plaatsvinden onder bepaalde voorwaarden die zijn vastgelegd in het rechtskader van het derde land[56].

60. In het kader van de Europese Unie omvatten deze voorwaarden bijvoorbeeld het verstrekken van specifieke informatie aan de betrokkene en het recht op menselijke tussenkomst door de verwerkingsverantwoordelijke, met name om zijn/haar standpunt kenbaar te maken, om uitleg te krijgen over het na een dergelijke beoordeling genomen besluit of om het besluit aan te vechten.

61. De wetgeving van het derde land moet in elk geval voorzien in de nodige waarborgen voor de rechten en vrijheden van de betrokkene. In dit verband moet ook rekening worden gehouden met het bestaan van een mechanisme om de bevoegde autoriteiten van de betrokken lidstaat in kennis te stellen van verdere verwerking, zoals het gebruik van de doorgegeven gegevens voor grootschalige profilering.

c) Gegevensbescherming door ontwerp en standaardinstellingen (artikel 20)

62. Bij de beoordeling van de adequaatheid moet aandacht worden besteed aan de verplichting voor verwerkingsverantwoordelijken om intern beleid vast te stellen en maatregelen uit te voeren die in overeenstemming zijn met de beginselen van gegevensbescherming door ontwerp en standaardinstellingen, rekening houdend met de stand van de techniek, de uitvoeringskosten en de aard, de reikwijdte, de context en de doeleinden van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, die aan de verwerking zijn verbonden, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, om passende technische en organisatorische maatregelen te nemen, zoals pseudonimisering, die zijn opgesteld met als doel de

[54] Deze bijzondere categorieën worden in overweging 37 van de richtlijn gegevensbescherming bij rechtshandhaving ook "gevoelige gegevens" genoemd.
[55] Dergelijke aanvullende waarborgen kunnen bijvoorbeeld specifieke veiligheidsmaatregelen zijn, beperkte toegangsrechten voor personeel, beperkingen met betrekking tot verdere verwerking, geautomatiseerde besluitvorming, verder delen of verdere doorgifte.
[56] Advies nr. 1/15, punt 173.

gegevensbeschermingsbeginselen, zoals gegevensminimalisatie, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen.

C. Procedurele en handhavingsmechanismen

63. Al kunnen de middelen waarmee het derde land voor waarborgen voor een passend beschermingsniveau kan zorgen, anders zijn dan die welke binnen de Europese Unie worden ingezet[57], een systeem dat verenigbaar is met het Europese systeem moet worden gekenmerkt door de volgende elementen:

a) Bevoegde onafhankelijke toezichthoudende autoriteit (artikel 36, lid 2, punt b), artikel 36, lid 3, en overweging 67)

64. Er moeten in het derde land een of meer onafhankelijke toezichthoudende autoriteiten zijn, die tot taak hebben de naleving van de bepalingen aangaande gegevensbescherming en bescherming van de persoonlijke levenssfeer te waarborgen en te handhaven. De toezichthoudende autoriteit is volledig onafhankelijk en onpartijdig in de uitvoering van haar taken en bevoegdheden en zij vraagt noch aanvaardt daarbij instructies. In dat verband moet de toezichthoudende autoriteit over alle passende handhavingsbevoegdheden beschikken om de naleving van de rechten op het gebied van gegevensbescherming effectief te waarborgen en om het bewustzijn hieromtrent te bevorderen. De personeelsbezetting en de begroting van de toezichthoudende autoriteit verdienen eveneens aandacht. De toezichthoudende autoriteit kan ook op eigen initiatief onderzoeken verrichten. Zij moet ook worden belast met het bijstaan en adviseren van betrokkenen bij de uitoefening van hun rechten (zie ook punt c hierna). In de adequaatheidsbesluiten moet in voorkomend geval de toezichthoudende autoriteit of autoriteiten en de mechanismen voor samenwerking met de toezichthoudende autoriteiten van de lidstaten om de gegevensbeschermingsregels te handhaven, worden vastgesteld.

b) Doeltreffende toepassing van de gegevensbeschermingsregels

65. Het systeem van een derde land moet garanderen dat verwerkingsverantwoordelijken en degenen die namens hen persoonsgegevens verwerken, zich sterk bewust zijn van hun verplichtingen, taken en bevoegdheden, en dat betrokkenen zich bewust zijn van hun rechten en de wijze waarop zij deze kunnen uitoefenen. Bij het handhaven van de naleving van de regels kunnen doeltreffende en afschrikkende sancties een belangrijke rol spelen, evenals, uiteraard, systemen voor rechtstreekse controle door autoriteiten.

66. Een gegevensbeschermingskader van een derde land moet verwerkingsverantwoordelijken of degenen die namens hen persoonsgegevens verwerken, verplichten zich aan dit kader te houden en te kunnen aantonen, met name aan de bevoegde toezichthoudende autoriteit, dat zij aan de regels voldoen. Dergelijke maatregelen moeten het gedurende een passende periode registreren van gegevensverwerkingsactiviteiten of het bijhouden van logbestanden daarvan omvatten. Zij kunnen ook bijvoorbeeld gegevensbeschermingseffectbeoordelingen, de aanstelling van een functionaris voor gegevensbescherming of gegevensbescherming door ontwerp en standaardinstellingen omvatten.

c) Het gegevensbeschermingssysteem vergemakkelijkt de uitoefening van de rechten van betrokkenen (artikelen 12, 17 en 46, richtlijn gegevensbescherming bij rechtshandhaving)

67. Een gegevensbeschermingskader van een derde land dient verwerkingsverantwoordelijken ertoe te verplichten de uitoefening van de in deel A, punt j), bedoelde rechten van betrokkenen te

[57] Schrems I, punt 74.

vergemakkelijken en te bepalen dat de toezichthoudende autoriteit van dat land de betrokkene desgevraagd informeert over de uitoefening van zijn of haar rechten[58].

d) Het systeem voor gegevensbescherming voorziet in passende verhaalmechanismen

68. Hoewel er momenteel geen rechtspraak is met betrekking tot de adequaatheid van een rechtsstelsel van een derde land in het kader van de richtlijn gegevensbescherming bij rechtshandhaving, heeft het Hof het grondrecht op doeltreffende rechterlijke bescherming uitgelegd zoals verankerd in artikel 47 van het Handvest. Artikel 47, eerste alinea, van het Handvest schrijft immers voor dat eenieder wiens door het recht van de EU gewaarborgde rechten en vrijheden zijn geschonden, recht heeft op een doeltreffende voorziening in rechte[59], met inachtneming van de in dat artikel gestelde voorwaarden.

69. Volgens vaste rechtspraak is het bestaan van effectieve rechterlijke toetsing om de naleving van de bepalingen van Unierecht te verzekeren, inherent aan het bestaan van een rechtsstaat. Een regeling die niet in enige beroepsmogelijkheid voor een persoon voorziet om toegang tot de hem betreffende persoonsgegevens te verkrijgen, of rectificatie of verwijdering van die gegevens, eerbiedigt de wezenlijke inhoud van het grondrecht op een effectieve voorziening in rechte zoals neergelegd in artikel 47 van het Handvest niet[60].

70. De betrokkene moet rechtsmiddelen kunnen aanwenden om zijn of haar rechten snel en doeltreffend, en zonder buitensporige kosten, te doen gelden en de naleving ervan te waarborgen.

71. Daartoe moeten er toezichtmechanismen zijn die het mogelijk maken klachten onafhankelijk te onderzoeken en eventuele inbreuken op het recht op gegevensbescherming en de eerbiediging van de persoonlijke levenssfeer vast te stellen en daadwerkelijk te bestraffen.

72. Wanneer de regels niet worden nageleefd, moet de betrokkene van wie de persoonsgegevens aan het derde land worden doorgegeven, in het derde land ook over doeltreffende administratieve en gerechtelijke beroepsmogelijkheden beschikken, onder meer voor vergoeding van de schade als gevolg van de onrechtmatige verwerking van zijn of haar persoonsgegevens. Dit is van het grootste belang en vereist onder meer een systeem van onafhankelijke rechtspleging of arbitrage dat schadeloosstelling en het opleggen van sancties, waar van toepassing, mogelijk maakt.

[58] De uitoefening van de rechten van betrokkenen kan direct of indirect zijn.
[59] Het Hof is van oordeel dat een doeltreffende rechterlijke bescherming niet alleen kan worden gewaarborgd door een rechterlijke instantie, maar ook door een orgaan dat garanties biedt die in wezen gelijkwaardig zijn aan die van artikel 47 van het Handvest (zie Schrems II, punt 197). Dit kan met name van belang zijn voor internationale organisaties.
[60] Schrems II, punten 187 en 194, en aldaar aangehaalde rechtspraak.