

Advies van de EDPB (artikel 70, lid 1, onder s)



Advies 5/2023 betreffende het ontwerp van uitvoeringsbesluit van de Europese Commissie inzake het passende niveau van bescherming van persoonsgegevens krachtens het EU-VS-kader voor gegevensbescherming

Vastgesteld op 28 februari 2023

Samenvatting

Op 13 december 2022 heeft de Europese Commissie een ontwerp van adequaatheidsbesluit (hierna “het ontwerpbesluit” genoemd) gepubliceerd dat bijlagen bevat die een nieuw kader vormen voor de trans-Atlantische uitwisseling van persoonsgegevens, het EU-VS-kader voor gegevensbescherming (Data Privacy Framework, hierna “DPF”), dat in de plaats moet komen van het vorige EU-VS-privacyschild, dat door het Hof van Justitie van de Europese Unie (hierna “het Hof”) op 16 juli 2020 in de zaak Schrems II ongeldig is verklaard. Het belangrijkste onderdeel van het DPF zijn de beginselen van het EU-VS-kader voor gegevensbescherming, inclusief de aanvullende beginselen (gezamenlijk “de DPF-beginselen”).

Overeenkomstig artikel 70, lid 1, punt s), van Verordening (EU) 2016/679¹ van het Europees Parlement en de Raad (hierna “AVG”) heeft de Commissie het advies van het Europees Comité voor gegevensbescherming (hierna “EDPB”) gevraagd over het ontwerpbesluit.

Het EDPB heeft op basis van het onderzoek van het ontwerpbesluit beoordeeld of het in de VS geboden beschermingsniveau adequaat is. Het EDPB heeft zowel de commerciële aspecten beoordeeld als de toegang tot persoonsgegevens die vanuit de EU worden doorgegeven en het gebruik daarvan door overheidsinstanties in de VS.

Het EDPB heeft rekening gehouden met het toepasselijke EU-rechtskader voor gegevensbescherming zoals vastgelegd in de AVG, alsook met het grondrecht op de eerbiediging van het privéleven en op de bescherming van persoonsgegevens zoals neergelegd in de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie en artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens. Het EDPB heeft ook rekening gehouden met het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht zoals neergelegd in artikel 47 van het Handvest, alsmede met de jurisprudentie in verband met de verschillende grondrechten.

Voorts heeft het EDPB de vereisten van de adequaatheidsreferentie, vastgesteld door het EDPB, in overweging genomen².

Het hoofddoel van het EDPB is de Commissie te adviseren over de adequaatheid van het beschermingsniveau voor natuurlijke personen wier persoonsgegevens aan de VS worden doorgegeven. Het is van belang te erkennen dat het EDPB niet verwacht dat het Amerikaanse kader voor gegevensbescherming identiek is aan de Europese gegevensbeschermingswetgeving.

Het EDPB herinnert er echter aan dat de wetgeving van het derde land slechts wordt geacht een adequaat beschermingsniveau te bieden als deze, zoals artikel 45 AVG en de rechtspraak van het Hof vereisen, de betrokkenen een beschermingsniveau biedt dat in feite overeenkomt met het niveau dat in de EU wordt verzekerd.

¹ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PBL 119 van 4.5.2016, blz. 1).

² Groep gegevensbescherming artikel 29, [Adequaatheidsreferentie, WP 254 rev.01, 28 november 2017, zoals laatst herzien en vastgesteld op 6 februari 2018, bekrachtigd door het EDPB op 25 mei 2018 \(hierna de “adequaatheidsreferentie” genoemd\)](#).

1.1. Algemene aspecten van gegevensbescherming

Het DPF bepaalt dat de naleving van de DPF-beginselen door DPF-organisaties in sommige gevallen kan worden beperkt (bv. voor zover nodig om te voldoen aan een rechterlijk bevel of om het algemeen belang te dienen). Om de effecten van deze vrijstellingen op het beschermingsniveau voor de betrokkenen beter in kaart te brengen, beveelt het EDPB aan dat de Commissie in het ontwerpbesluit een verduidelijking opneemt over de reikwijdte van de vrijstellingen, met inbegrip van de toepasselijke waarborgen krachtens het recht van de VS.

Het EDPB merkt op dat de structuur van de bijlagen en de nummering ervan de informatie nogal moeilijk te vinden en te raadplegen maakt. Dit draagt bij tot een algemene complexe presentatie van het nieuwe kader, met in de bijlagen een verzameling documenten van verschillende juridische waarde, en is wellicht niet bevorderlijk voor een goed begrip van de DPF-beginselen door betrokkenen, DPF-organisaties en EU-autoriteiten voor gegevensbescherming. Het EDPB benadrukt tevens dat de terminologie in het gehele DPF consistent moet worden gebruikt. Ook ontbreekt de definitie van een aantal essentiële termen³.

Het EDPB verwelkomt de updates van de DPF-beginselen⁴, die het bindende juridische kader zullen vormen voor DPF-organisaties, maar merkt op dat ondanks een aantal wijzigingen en aanvullende toelichtingen in de overwegingen van het ontwerpbesluit, de DPF-beginselen waaraan de DPF-organisaties zich moeten houden in wezen ongewijzigd blijven ten opzichte van de beginselen die van toepassing zijn in het kader van het privacyschild (waarop de jaarlijkse gezamenlijke evaluaties van de Groep gegevensbescherming artikel 29 en het EDPB waren gebaseerd). De DPF-beginselen zijn ook grotendeels dezelfde als die van het ontwerp-privacyschild waarop de Groep gegevensbescherming artikel 29 haar advies van 2016 heeft gebaseerd⁵. Voor de DPF-beginselen die grotendeels ongewijzigd zijn, acht het EDPB het niet nodig alle eerder door de Groep gegevensbescherming artikel 29 gemaakte opmerkingen te herhalen. Het EDPB heeft besloten zich te concentreren op specifieke aspecten die hij vandaag nog relevanter acht, gezien de evolutie van de juridische en technologische omgeving.

Het EDPB merkt bijvoorbeeld op dat sommige punten van zorg die eerder door de Groep gegevensbescherming artikel 29 en het EDPB met betrekking tot de beginselen van het privacyschild aan de orde zijn gesteld, nog steeds gelden. Deze betreffen met name de rechten van de betrokkenen (bv. sommige uitzonderingen op het recht van toegang en het tijdschema en de modaliteiten voor het recht om bezwaar te maken), het ontbreken van essentiële definities, het gebrek aan duidelijkheid met betrekking tot de toepassing van de DPF-beginselen op verwerkers, en de ruime vrijstelling voor openbaar beschikbare informatie⁶.

Het EDPB wenst tevens te herhalen dat het beschermingsniveau van natuurlijke personen wier gegevens worden doorgegeven, niet mag worden ondermijnd door verdere doorgiften door de eerste ontvanger van de doorgegeven gegevens⁷. Het EDPB verzoekt de Commissie nogmaals te verduidelijken dat de waarborgen die door de eerste ontvanger aan de importeur in het derde land

³ Dit is het geval voor de termen “vertegenwoordiger” en “verwerker”. Bovendien moet het begrip “personeelsgegevens” nog met de Amerikaanse autoriteiten worden besproken.

⁴ Bijvoorbeeld de verduidelijking dat versleutelde gegevens persoonsgegevens zijn.

⁵ [Advies 01/2016 van de Groep gegevensbescherming artikel 29 inzake het ontwerpbesluit over de adequaatheid van het Europees-Amerikaanse privacyschild, vastgesteld op 13 april 2016 \(hierna “Advies 01/2016 van de Groep gegevensbescherming artikel 29” genoemd\).](#)

⁶ EU-VS-privacyschild — derde jaarlijkse gezamenlijke evaluatie, EDPB-verslag vastgesteld op 12 november 2019, punt 11.

⁷ AVG-adequaateitsreferentie, hoofdstuk 3, punt A, 9).

worden opgelegd doeltreffend moeten zijn in het licht van de wetgeving van het derde land, voordat een verdere doorgifte in het kader van het DPF plaatsvindt.

De snelle ontwikkelingen op het gebied van geautomatiseerde besluitvorming en profilering — in toenemende mate door middel van AI-technologieën — vereisen bijzondere aandacht. Het EDPB is ingenomen met de verwijzingen van de Commissie naar specifieke waarborgen waarin de desbetreffende Amerikaanse wetgeving op verschillende gebieden voorziet⁸. Het beschermingsniveau voor natuurlijke personen lijkt echter te variëren naargelang van de eventuele sectorspecifieke regels die op de betrokken situatie van toepassing zijn. Het EDPB stelt dat specifieke regels inzake geautomatiseerde besluitvorming nodig zijn om voldoende waarborgen te bieden, waaronder het recht van de betrokkene om de betrokken logica te kennen, het besluit aan te vechten en menselijke tussenkomst te verkrijgen wanneer het besluit hem of haar in aanzienlijke mate raakt.

Het EDPB herinnert aan het belang van doeltreffend toezicht op en handhaving van het DPF en is van oordeel dat nalevingscontroles met betrekking tot meer materiële vereisten van cruciaal belang zijn. Deze aspecten zullen door het EDPB nauwlettend worden gevolgd, onder meer in het kader van de periodieke evaluaties. Het EDPB neemt kennis van de hernieuwde toezeggingen in de brieven van de Federal Trade Commission (hierna “FTC”)⁹ en het Department of Transportation (ministerie van Vervoer)¹⁰ met betrekking tot de handhaving, bijvoorbeeld om prioriteit te geven aan het onderzoek van vermeende schendingen van het DPF.

Het EDPB merkt op dat er zeven verhaalsmogelijkheden zijn voor betrokkenen in de EU, indien hun persoonsgegevens in strijd met het DPF worden verwerkt. Deze verhaalmechanismen zijn dezelfde als die in het vroegere privacyschild, waarover de Groep gegevensbescherming artikel 29 opmerkingen had gemaakt¹¹. De doeltreffendheid van deze verhaalmechanismen zal door het EDPB nauwlettend worden gevolgd, onder meer in het kader van de periodieke evaluaties.

1.2. Toegang tot persoonsgegevens die vanuit de Europese Unie worden doorgegeven en het gebruik daarvan door overheidsinstanties in de VS

In het ontwerpbesluit concludeert de Europese Commissie dat elke inmenging in het algemeen belang, met name ten behoeve van de handhaving van het strafrecht en de nationale veiligheid, door overheidsinstanties van de VS in de grondrechten van de natuurlijke personen wier persoonsgegevens uit de Unie aan de Verenigde Staten worden doorgegeven op grond van het EU-VS-kader voor gegevensbescherming, beperkt zal blijven tot wat strikt noodzakelijk is om de betrokken legitieme doelstelling te bereiken, en dat er doeltreffende rechtsbescherming tegen dergelijke inmenging bestaat¹².

De Europese Commissie komt tot haar conclusie na een uitgebreide beoordeling van Executive Order 14086 tot verbetering van de waarborgen voor activiteiten van de VS op het gebied van signals intelligence (SIGINT — inlichtingen uit het berichtenverkeer) (Presidentieel Besluit 14086, hierna “EO 14086”). EO 14086 werd op 7 oktober 2022 door de Amerikaanse president uitgevaardigd, na onderhandelingen van de Europese Commissie met de Amerikaanse regering in de nasleep van de ongeldigverklaring van het vorige adequaatheidsbesluit, het zogenaamde privacyschild, door het Hof van Justitie van de Europese Unie (het Hof).

⁸ Ontwerpbesluit, overweging 35.

⁹ Ontwerpbesluit, bijlage IV.

¹⁰ Ontwerpbesluit, bijlage V.

¹¹ Zie met name Advies 01/2016 van de Groep gegevensbescherming artikel 29, punt 2.2.6, a).

¹² Ontwerpbesluit, overweging 195.

Het EDPB zou graag zien dat niet alleen de inwerkingtreding maar ook de vaststelling van het besluit afhankelijk wordt gesteld van onder meer de vaststelling van geactualiseerde beleidsmaatregelen en procedures door alle Amerikaanse inlichtingendiensten ter uitvoering van EO 14086. Het EDPB beveelt de Commissie aan deze geactualiseerde beleidsmaatregelen en procedures te beoordelen en deze beoordeling met het EDPB te delen.

Wat de toegang van de overheid tot aan de VS overgedragen persoonsgegevens betreft, heeft het EDPB zijn analyse toegespitst op de beoordeling van het nieuwe EO 14086, aangezien dit effectief bedoeld is om de door het Hof in zijn arrest Schrems II vastgestelde tekortkomingen aan te pakken en te verhelpen toen het Hof het vorige adequaatheidsbesluit ongeldig verklaarde.

Het EDPB erkent dat het Amerikaanse rechtskader voor activiteiten op het gebied van SIGINT is gewijzigd door de vaststelling van EO 14086 en beschouwt de in dit besluit opgenomen aanvullende waarborgen als een aanzienlijke verbetering. EO 14086 introduceert de begrippen noodzakelijkheid en evenredigheid in het Amerikaanse rechtskader voor SIGINT, en voorziet, indien de EU wordt aangewezen als in aanmerking komende regionale organisatie voor economische integratie, in een nieuw verhaalmechanisme voor natuurlijke personen uit de EU. Het EDPB meent dat het nieuwe verhaalmechanisme een aanzienlijke verbetering is ten opzichte van het vorige zogenoemde ombudsmanmechanisme in het kader van het privacyschild. In tegenstelling tot het vorige rechtskader, dat geen rechten voor natuurlijke personen uit de EU creëerde, zoals het Hof uitdrukkelijk heeft opgemerkt, creëert het nieuwe EO 14086 dergelijke rechten wel, en biedt het meer waarborgen voor de onafhankelijkheid van de Data Protection Review Court (toetsingsinstantie voor gegevensbescherming van de Verenigde Staten, hierna “DPRC”) en doeltreffender bevoegdheden om schendingen te verhelpen.

Bij een vergelijking van de in EO 14086 opgenomen aanvullende waarborgen met wat het EDPB heeft aangemerkt als de Europese essentiële garanties, als de standaard die is uitgewerkt op basis van de jurisprudentie van het Hof en het Europees Hof voor de Rechten van de Mens (hierna “EHRM”), heeft het EDPB in zijn beoordeling nog een aantal punten aangestipt die verder moeten worden verduidelijkt, aandacht verdienen of aanleiding geven tot bezorgdheid. Uit deze punten blijkt dat, hoewel het EDPB zijn advies heeft gebaseerd op het arrest Schrems II, de reikwijdte van de beoordeling van het EDPB noodzakelijkerwijs overwegingen omvat die verder gaan dan de specifieke bevindingen in het arrest Schrems II.

Het EDPB meent dat met name kwesties in verband met “tijdelijke bulksgewijze verzameling” en de verdere bewaring en verspreiding van de (bulksgewijs) verzamelde gegevens in het rechtskader van de VS verdere verduidelijking behoeven.

Aangezien de toetsing van de essentiële gelijkwaardigheid geen toetsing van het identieke karakter is, en aangezien de waarborgen in het nieuwe rechtskader inzake SIGINT zijn versterkt, richt het EDPB zijn aandacht vooral op een beoordeling van de waarborgen in hun geheel, volgens een holistische aanpak die de waarborgen voor de gehele verwerkingscyclus omvat, van het verzamelen van gegevens tot de verspreiding van gegevens, en met inbegrip van de elementen toezicht en verhaal.

In dit verband benadrukt het EDPB de volgende bevindingen:

hoewel het EDPB erkent dat met EO 14086 de begrippen noodzakelijkheid en evenredigheid in het rechtskader voor SIGINT worden geïntroduceerd, onderstreept hij de noodzaak om de gevolgen van deze wijzigingen in de praktijk nauwlettend te volgen, met inbegrip van de evaluatie van de interne beleidsmaatregelen en procedures ter uitvoering van de waarborgen van het EO op het niveau van de instanties.

Het EDPB is ook ingenomen met het feit dat EO 14086 een lijst van specifieke doeleinden bevat waarvoor gegevens wel en niet kunnen worden verzameld, waarbij wordt opgemerkt dat de doelstellingen kunnen worden geactualiseerd met aanvullende — niet noodzakelijk openbare — doelstellingen in het licht van nieuwe eisen in verband met de nationale veiligheid.

Een tekortkoming in het huidige kader is volgens het EDPB dat in het Amerikaanse rechtskader, wanneer de bulksgewijze verzameling krachtens Executive Order 12333 wordt toegestaan, het vereiste van voorafgaande toestemming door een onafhankelijke autoriteit ontbreekt, terwijl die toestemming in de recentste jurisprudentie van het EHRM wordt vereist, en dat het Amerikaanse rechtskader evenmin voorziet in een systematische onafhankelijke toetsing achteraf door een rechtbank of een gelijkwaardig onafhankelijk orgaan. Wat betreft de voorafgaande onafhankelijke toestemming voor surveillance op grond van sectie 702 FISA betreurt het EDPB dat de Foreign Intelligence Surveillance Court (rechtbank voor surveillance op buitenlandse inlichtingen, hierna “FISC”) een programma-aanvraag niet toetst op naleving van EO 14086 bij de certificering van het programma dat op niet-Amerikanen gerichte gegevensverzameling toelaat, ook al zijn de inlichtingendiensten die het programma uitvoeren daaraan gebonden. Volgens het EDPB moeten de in dit EO vervatte aanvullende waarborgen niettemin in aanmerking worden genomen, ook door de FISC. Het EDPB herinnert eraan dat verslagen van de Privacy and Civil Liberties Oversight Board (raad van toezicht op de privacy en de burgerlijke vrijheden, hierna “PCLOB”) bijzonder nuttig zouden zijn om te beoordelen hoe de waarborgen van EO 14086 zullen worden uitgevoerd en hoe deze waarborgen worden toegepast wanneer gegevens worden verzameld uit hoofde van sectie 702 FISA en EO 12333.

Wat het verhaalmechanisme betreft, erkent het EDPB de aanzienlijke verbeteringen met betrekking tot de bevoegdheden van de Data Protection Review Court (“DPRC”) en de grotere onafhankelijkheid daarvan in vergelijking met de ombudsman. Het EDPB erkent ook de aanvullende waarborgen waarin het nieuwe verhaalmechanisme voorziet, zoals de rol van de bijzondere juristen (*special advocates*) die onder meer de belangen van de klager behartigen evenals de toetsing van het verhaalmechanisme door de PCLOB. Rekening houdend met de aard van de nationale veiligheid en de waarborgen van EO 14086, is het EDPB niettemin bezorgd over de algemene toepassing van het standaardantwoord van de DPRC waarin de klager wordt meegedeeld dat ofwel geen onder EO 14086 vallende schendingen zijn vastgesteld, ofwel een besluit is genomen dat passende herstelmaatregelen vereist, en de onmogelijkheid om daartegen hoger beroep in te stellen, in hun geheel genomen. Gezien het belang van het verhaalmechanisme roept het EDPB de Commissie op de praktische werking van dit mechanisme nauwlettend te volgen.

Het EDPB verwacht dat de Commissie gevolg zal geven aan haar toezegging om het adequaatheidsbesluit op te schorten, in te trekken of te wijzigen om redenen van urgentie, met name indien de Amerikaanse uitvoerende macht zou besluiten de in de EO opgenomen waarborgen te beperken¹³.

In het algemeen is het EDPB positief over de aanzienlijke verbeteringen die het EO biedt ten opzichte van het vorige rechtskader, met name wat betreft de invoering van de beginselen van noodzakelijkheid en evenredigheid en het individuele verhaalmechanisme voor betrokkenen uit de EU. Gezien de punten van zorg die werden aangekaart en de verduidelijkingen die werden gevraagd, stelt het EDPB voor dat deze punten van zorg worden weggenomen en dat de Commissie de gevraagde verduidelijkingen verstrekt om de gronden voor het ontwerpbesluit te onderbouwen en om bij de

¹³ Ontwerpbesluit, overweging 212.

toekomstige gezamenlijke evaluaties nauwlettend toe te zien op de concrete uitvoering van dit nieuwe rechtskader, met name op de waarborgen die het biedt.

Inhoudsopgave

1	INLEIDING.....	10
1.1	Kader voor gegevensbescherming van de VS.....	10
1.2	Reikwijdte van de beoordeling van het EDPB	12
1.3	Algemene opmerkingen en punten van zorg	14
1.3.1	Beoordeling van het interne recht	14
1.3.2	Internationale toezeggingen van de VS.....	14
1.3.3	Vooruitgang op het gebied van wetgeving inzake gegevensbescherming in de VS	15
1.3.4	Toepassingsgebied van het ontwerpbesluit	16
1.3.5	Beperkingen op de verplichting tot naleving van de DPF-beginselen	16
1.3.6	Wijzigingen met betrekking tot het “privacyschild”	17
1.3.7	Gebrek aan duidelijkheid in de documenten van het DPF	17
2	ALGEMENE ASPECTEN VAN GEGEVENSBESCHERMING.....	18
2.1	Inhoudelijke beginselen	18
2.1.1	Begrippen	18
2.1.2	Het beginsel van doelbinding	18
2.1.3	Recht van inzage, rectificatie, wissing en bezwaar.....	19
2.1.4	Beperkingen ten aanzien van verdere doorgifte.....	20
2.1.5	Geautomatiseerde besluitvorming en profilering	22
2.2	Procedurale en handavingsmechanismen	23
2.3	Verhaalmechanismen.....	24
3	TOEGANG TOT PERSOONSgegevens die vanuit de Europese Unie worden doorgegeven en het gebruik daarvan door overheidsinstanties in de VS.....	25
3.1	Toegang en gebruik met het oog op handhaving van het strafrecht.....	25
3.1.1	De toegang van rechtshandavingsinstanties tot persoonsgegevens moet gebaseerd zijn op duidelijke, nauwkeurige en toegankelijke regels.....	25
3.1.2	De noodzakelijkheid en evenredigheid van de nagestreefde legitieme doelstellingen moeten worden aangetoond	26
3.1.3	Er moet een onafhankelijk toezichtmechanisme bestaan	28
3.1.4	De betrokken personen moeten beschikken over doeltreffende beroepsmogelijkheden..	28
3.1.5	Verder gebruik van de verzamelde informatie	29
3.2	Toegang en gebruik ten behoeve van de nationale veiligheid	30
3.2.1	Garantie A — De verwerking moet in overeenstemming zijn met de wet en gebaseerd zijn op duidelijke, nauwkeurige en toegankelijke regels	31
3.2.2	Garantie B — De noodzakelijkheid en evenredigheid van de nagestreefde legitieme doelstellingen moeten worden aangetoond.....	35

3.2.3	Garantie C — Toezicht	46
3.2.4	Garantie D — Personen moeten over doeltreffende voorzieningen in rechte beschikken	51
4	UITVOERING VAN EN MONITORING OP HET ONTWERPBESLUIT	60

Het Europees Comité voor gegevensbescherming

Het Europees Comité voor gegevensbescherming heeft de volgende verklaring aangenomen:

Gezien artikel 70, lid 1, punt s), van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna “AVG” genoemd)¹,

Gezien de EER-overeenkomst en in het bijzonder bijlage XI en protocol 37 bij die overeenkomst, als gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018²,

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

BRENGT HET VOLGENDE ADVIES UIT

1 INLEIDING

1.1 Kader voor gegevensbescherming van de VS

1. De Verenigde Staten (“VS”) en de Europese Unie (“EU”) benaderen privacy en gegevensbescherming op verschillende manieren. Terwijl privacy en gegevensbescherming in de EU grondrechten zijn die worden gewaarborgd in de artikelen 7 en 8 van het Europees Handvest van de grondrechten, wordt gegevensbescherming in de VS doorgaans benaderd vanuit het oogpunt van consumentenbescherming. Bijgevolg verschillen de regelgevingsbenaderingen in de VS en de EU³.
2. Anders dan de alomvattende aanpak van de EU in de AVG, bestaat er in de VS geen alomvattende algemene wet inzake gegevensbescherming op federaal niveau. De bescherming van de privacy in de VS vindt veeleer plaats via een sectorale aanpak en een aanpak op het niveau van de staten. Zo vallen sommige specifieke sectoren onder specifieke wetten, bv.:
 - de Health Insurance Portability and Accountability Act (wet overdraagbaarheid en verantwoordingsplicht gezondheidsverzekering, hierna “HIPAA”)⁴;

¹Verordening (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) (Voor de EER relevante tekst), PBL 119 van 4.5.2016, blz. 1.

² Met “lidstaten” worden in dit advies “lidstaten van de EER” bedoeld.

³ Zie ook het ontwerp van uitvoeringsbesluit van de Europese Commissie uit hoofde van Verordening (EU) 2016/679 van het Europees Parlement en de Raad inzake het passende niveau van bescherming van persoonsgegevens krachtens het EU-VS-kader voor gegevensbescherming, bekendgemaakt op 13 december 2022 (hierna: het “ontwerpbesluit”), bijlage I, hoofdstuk I.

⁴ De Health Insurance Portability and Accountability Act van 1996 (HIPAA) is een federale wet van de Verenigde Staten. Met deze wet worden nationale normen in het leven geroepen om de gevoelige gezondheidsinformatie van patiënten te beschermen. De HIPAA heeft tot doel de gezondheidsinformatie van personen adequaat te

- de Children's Online Privacy Protection Act (wet bescherming online privacy van kinderen, hierna "COPPA")⁵;
- de Gramm-Leach-Bliley Act (Wet Gramm-Leach-Bliley)⁶.

3. Op het gebied van overheidstoegang tot persoonsgegevens die vanuit de EU aan de VS worden doorgegeven, gelden een aantal verschillende rechtsgrondslagen, beperkingen en waarborgen. De juridische procedures voor toegang tot informatie voor rechtshandavingsdoeleinden vloeien ofwel rechtstreeks voort uit de grondwet van de Verenigde Staten (het vierde amendement), uit de gewone wetten en het procesrecht of uit de richtsnoeren en de beleidsmaatregelen van het ministerie van Justitie op federaal niveau of op het niveau van de staten. De toegang tot informatie ten behoeve van de nationale veiligheid wordt geregeld door verscheidene rechtsinstrumenten en met name door de Foreign Intelligence Surveillance Act ("FISA") (wet betreffende de surveillance op buitenlandse inlichtingen), Executive Order 12333, het onlangs aangenomen Executive Order 14086 en het decreet van de Attorney General (minister van Justitie)⁷ tot oprichting van een rechtbank voor toetsing van de gegevensbescherming (Data Protection Review Court, "DPRC").
4. Op 13 december 2022 heeft de Commissie haar ontwerp van uitvoeringsbesluit uit hoofde van Verordening (EU) 2016/679 van het Europees Parlement en de Raad inzake het passende niveau van bescherming van persoonsgegevens krachtens het EU-VS-kader voor gegevensbescherming ("het ontwerpbesluit") uitgebracht, dat in de bijlage het EU-VS-kader voor gegevensbescherming (het "DPF") bevat. Om de hierboven uiteengezette redenen is het ontwerpbesluit niet gebaseerd op een specifiek en alomvattend federaal juridisch kader, maar op het DPF.
5. Het DPF werkt als volgt: het Amerikaanse ministerie van Handel ("het ministerie") vaardigt de EU-VS-kaderbeginselen inzake gegevensbescherming uit, met inbegrip van de aanvullende beginselen (samen

beschermen, terwijl gezondheidsinformatie mag worden doorgegeven voor de verstrekking en bevordering van gezondheidszorg van hoge kwaliteit. De HIPAA regelt het gebruik en de openbaarmaking van gezondheidsinformatie door entiteiten die onder de Privacy Rule (regelgeving inzake persoonsgegevens) vallen. Zij bevat ook normen voor de rechten van natuurlijke personen om inzicht te krijgen in het gebruik van hun gezondheidsinformatie en dat gebruikte controleren.

<https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>; <https://www.justice.gov/opcl/privacy-act-1974>

⁵ Het voornaamste doel van de COPPA is ouders zeggenschap te geven over welke persoonsgegevens van hun kinderen onder de 13 jaar worden verzameld door exploitanten van op kinderen gerichte websites en onlinediensten (waaronder mobiele apps en IoT-apparaten, zoals slim speelgoed) of websites voor het algemene publiek. De COPPA vereist dat deze exploitanten de ouders in kennis te stellen en verifieerbare toestemming van de ouders verkrijgen. Dit geldt ook voor gegevens van buitenlandse kinderen als de websites of diensten in de VS worden geëxploiteerd en onder de COPPA vallen. Tegelijkertijd is de regelgeving ook van toepassing op in het buitenland gevestigde websites en diensten indien deze gericht zijn op kinderen in de VS. Zie: <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions> en ontwerpbesluit, bijlage IV, blz. 3.

⁶ Een van de doelstellingen van de Gramm-Leach-Bliley Act is de bescherming van de privacy van de consument in de financiële sector. De Gramm-Leach-Bliley Act vereist dat financiële instellingen hun klanten uitleg geven over hun informatie-uitwisselingspraktijken en waarborgen creëren om klanteninformatie te beschermen (bv. voor bedrijven die door de FTC worden gereguleerd krachtens de FTC-regelgeving inzake waarborgen ("FTC Safeguards Rule")). <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>

⁷ Attorney General Order nr. 5517-2022, tot wijziging van de voorschriften ("regulations") van het ministerie van Justitie van de VS, zoals toegestaan en opgedragen bij EO 14086.

“de beginselen”) en bijlage I bij de beginselen (“bijlage I”), uit hoofde van zijn wettelijke bevoegdheid om de internationale handel te bevorderen en te ontwikkelen (15 U.S.C. § 1512)⁸.

6. De uitwerking van de “beginselen” (de “DPF-beginselen”) vond plaats in overleg met de Europese Commissie (de “Commissie”), het bedrijfsleven en andere belanghebbenden teneinde de handel tussen de EU en de VS te vergemakkelijken⁹ en er tegelijkertijd voor te zorgen dat de betrokkenen een beschermingsniveau wordt geboden dat in wezen gelijkwaardig is aan het niveau dat in de EU wordt gewaarborgd.
7. De DPF-beginselen worden beschreven als een “cruciaal onderdeel” van het DPF. Enerzijds bieden zij een “gebruiksklaar mechanisme” voor de doorgifte van gegevens van de EU naar de VS. Anderzijds worden persoonsgegevens die van de EU naar de VS worden doorgegeven, beveiligd en beschermd overeenkomstig het Unierecht.
8. Het DPF is alleen van toepassing op organisaties in de VS die zichzelf hebben gecertificeerd volgens de eisen van het kader (“DPF-organisaties”). Voorlopig is dit alleen mogelijk indien zij onder de jurisdictie van de Federal Trade Commission (“FTC”) of het ministerie van Vervoer vallen. In de toekomst kunnen andere wettelijke instanties — die bevoegd zijn om toezicht te houden op de uitvoering van de DPF-beginselen — in een toekomstige bijlage worden toegevoegd.
9. In de DPF-beginselen wordt uiteengezet dat de voorwaarden van het kader kunnen worden afgedwongen door i) de FTC krachtens sectie 5 van de wet inzake de Federal Trade Commission (“FTC-wet”) die oneerlijke of misleidende handelingen in of met betrekking tot de handel verbiedt¹⁰, ii) het ministerie van Vervoer krachtens 49 U.S.C. § 41712 waarin het luchtvaartmaatschappijen of reisbureaus wordt verboden zich in te laten met oneerlijke of misleidende praktijken bij de verkoop van luchtvervoer, of iii) krachtens andere wet- en regelgeving waarbij dergelijke handelingen verboden zijn.
10. In de DPF-beginselen wordt erop gewezen dat noch de AVG in haar toepassing wordt aangetast, noch bestaande privacyverplichtingen, die anders krachtens het recht van de VS worden toegepast, door de DPF-beginselen worden beperkt.

1.2 Reikwijdte van de beoordeling van het EDPB

11. Het ontwerpbesluit weerspiegelt de beoordeling van het DPF door de Commissie, die het resultaat is van besprekingen met de Amerikaanse regering. Overeenkomstig artikel 70, lid 1, punt s), AVG wordt verwacht dat het EDPB advies uitbrengt over de bevindingen van de Commissie betreffende de adequaatheid van het beschermingsniveau in een derde land en, indien nodig, voorstellen tracht te doen om eventuele problemen aan te pakken.
12. Het EDPB verwelkomt de actualisering van de DPF-beginselen¹¹, die het bindende juridische kader voor DPF-organisaties zullen vormen. Het EDPB merkt echter op dat de DPF-beginselen in wezen dezelfde blijven als die van het privacyschild¹² (waarop de jaarlijkse gezamenlijke evaluaties van de Groep

⁸ Ontwerpbesluit, bijlage I, hoofdstuk I.

⁹ Zie vorige voetnoot.

¹⁰ 15 U.S.C. § 45, (a).

¹¹ Bijvoorbeeld de verduidelijking dat versleutelde gegevens persoonsgegevens zijn.

¹² Uitvoeringsverordening (EU) 2016/1250 van de Commissie van 12 juli 2016 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de gepastheid van de door het EU-VS-privacychild geboden bescherming, PBL 207, 1.8.2016, blz. 1.

gegevensbescherming artikel 29 en het EDPB waren gebaseerd). De DPF-beginselen zijn ook grotendeels dezelfde als die van het ontwerp-privacyschild waarop de Groep gegevensbescherming artikel 29 haar advies van 2016¹³ (“advies 01/2016 van de Groep gegevensbescherming artikel 29”) heeft gebaseerd. Voor de DPF-beginselen die grotendeels ongewijzigd zijn, acht het EDPB het niet nodig alle eerder door de Groep gegevensbescherming artikel 29 gemaakte opmerkingen te herhalen. Het EDPB heeft besloten zich te concentreren op specifieke aspecten die hij vandaag nog relevanter acht, gezien de evolutie van de juridische en technologische omgeving.

13. In overeenstemming met de jurisprudentie van het Hof¹⁴ heeft een zeer belangrijk deel van de analyse bovendien betrekking op de wettelijke regeling inzake de toegang van de overheid tot persoonsgegevens die aan de VS zijn doorgegeven.
14. Bij zijn beoordeling heeft het EDPB rekening gehouden met het toepasselijke Europese kader voor gegevensbescherming, waaronder de artikelen 7, 8 en 47 van het EU-Handvest van de grondrechten (“het Handvest”), die respectievelijk het recht op eerbiediging van het privéleven en van het familie- en gezinsleven, het recht op bescherming van persoonsgegevens en het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht beschermen, en artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens (“EVRM”), dat het recht op eerbiediging van het privé-, familie- en gezinsleven beschermt. Naast het bovenstaande heeft het EDPB de vereisten van de AVG, de relevante jurisprudentie en de door het EDPB vastgestelde adequaatheidsreferentie (“de AVG-adequaatheidsreferentie”) in overweging genomen¹⁵.
15. Deze exercitie heeft tot doel de Europese Commissie te voorzien van een advies over de beoordeling van de adequaatheid van het beschermingsniveau dat door het DPF wordt geboden. Het begrip “passend beschermingsniveau” werd al gehanteerd in Richtlijn 95/46/EG en is verder uitgewerkt door het Hof. Daarom is het belangrijk te herinneren aan de standaard die het Hof heeft vastgesteld in zijn arresten Schrems I¹⁶ (ongeldigverklaring van de “Veilige haven”) en Schrems II¹⁷ (ongeldigverklaring van het privacyschild).
16. In het arrest Schrems I heeft het Hof heeft gesteld dat, hoewel het “beschermingsniveau” in het derde land “in grote lijnen” moet overeenkomen met het in de EU gewaarborgde niveau, “de middelen waarmee dat derde land voor waarborgen voor een passend beschermingsniveau kan zorgen, anders [kunnen] zijn dan die welke binnen de Unie worden ingezet”¹⁸. Het doel is dus niet de Europese wetgeving punt voor punt te kopiëren, maar de grote lijnen en de kernvereisten van de wetgeving in kwestie vast te stellen. Adequaatheid kan worden bereikt door een combinatie van rechten voor de betrokkenen, verplichtingen voor verwerkers van persoonsgegevens of

¹³ Advies 01/2016 van de Groep gegevensbescherming artikel 29 inzake het ontwerpbesluit over de adequaatheid van het Europees-Amerikaanse privacyschild, vastgesteld op 13 april 2016 (hierna het “advies 01/2016 van de Groep gegevensbescherming artikel 29” genoemd).

¹⁴ Met name: arrest van het Hof van Justitie van 6 oktober 2015, Maximilian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, en arrest van het Hof van Justitie van 16 juli 2020, Data Protection Commissioner/Facebook Ireland Limited en Maximilian Schrems, C-311/18, ECLI:EU:C:2020:559.

¹⁵ Groep gegevensbescherming artikel 29, [Adequaatheidsreferentie, WP 254 rev.01, 28 november 2017, zoals laatst herzien en vastgesteld op 6 februari 2018, bekrachtigd door het EDPB op 25 mei 2018 \(hierna de “AVG-adequaatheidsreferentie” genoemd\)](#).

¹⁶ Arrest van het Hof van Justitie van 6 oktober 2015, Maximilian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 (hierna het “arrest Schrems I van het Hof” genoemd).

¹⁷ Arrest van het Hof van Justitie van 16 juli 2020, Data Protection Commissioner/Facebook Ireland Limited en Maximilian Schrems, C-311/18, ECLI:EU:C:2020:559 (hierna het “arrest Schrems II van het Hof” genoemd).

¹⁸ Arrest Schrems I van het Hof, punten 73-74.

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 regelgeving te waarborgen. Voor de doeltreffendheid van regelgeving voor gegevensbescherming zijn efficiënte handhavingsmechanismen van eminent belang¹⁹.

17. In zijn arrest Schrems II heeft het Hof geoordeeld dat de wetten op basis waarvan de Amerikaanse inlichtingendiensten toegang hebben tot aan de VS overgedragen persoonsgegevens (sectie 702 FISA/EO 12333) de in de artikelen 7 en 8 van het Handvest neergelegde rechten onevenredig beperken en dus niet zodanig zijn afgebakend dat wordt voldaan aan vereisten die in grote lijnen overeenkomen met die welke in het Unierecht worden gesteld door artikel 52, lid 1, tweede volzin, van het Handvest²⁰.
18. Bovendien stelde het Hof dat het vroegere rechtskader geen garanties bood die in wezen gelijkwaardig waren aan die welke door artikel 47 van het Handvest worden geëist, aangezien het ombudsmanmechanisme geen compensatie kon bieden voor het feit dat noch PPD-28 noch EO 12333 aan niet-Amerikanen een doeltreffende voorziening in rechte biedt²¹. De ombudsman was niet onafhankelijk van de uitvoerende macht en niet bevoegd om bindende besluiten te nemen ten aanzien van de Amerikaanse inlichtingendiensten²².
19. Bij EO 14086, dat PPD-28 in grote lijnen vervangt, zijn in het Amerikaanse recht twee nieuwe eisen ingevoerd die aansluiten bij het arrest Schrems II van het Hof: enerzijds dat SIGINT-activiteiten alleen mogen worden verricht voor zover dat nodig is om een gevalideerde prioritaire inlichtingenverzameling te bevorderen en alleen voor zover en op een wijze die evenredig is aan de gevalideerde inlichtingenprioriteit; en anderzijds een verhaalmechanisme.
20. In dit advies beoordeelt het EDPB met name in hoeverre het DPF en het onlangs aangenomen EO 14086 effectief tegemoetkomen aan de bevindingen van het Hof in zijn arrest.

1.3 Algemene opmerkingen en punten van zorg

1.3.1 Beoordeling van het interne recht

21. Het EDPB begrijpt dat de beoordeling in het ontwerpbesluit betrekking heeft op de DPF-beginselen. Niettemin zou het EDPB graag enige informatie ontvangen over de Amerikaanse juridische context waarin de DPF-organisaties actief zijn. Dit zou een beter begrip van de interactie van het DPF met de Amerikaanse wetgeving mogelijk maken. Zo wordt in bijlage I, hoofdstuk 1²³, bepaald dat de DPF-beginselen de verplichtingen inzake de bescherming van de persoonlijke levenssfeer niet beperken die anders krachtens de Amerikaanse wetgeving van toepassing zijn, zonder dat deze verplichtingen worden beschreven.

1.3.2 Internationale toezeggingen van de VS

22. Overeenkomstig artikel 45, lid 2, punt c), AVG en de AVG-adequaateitsreferentie moet de Europese Commissie bij de beoordeling van de adequaatheid van het beschermingsniveau van een derde land

¹⁹ AVG-adequaateitsreferentie, blz. 2.

²⁰ Arrest Schrems II van het Hof, punten 184-185.

²¹ Arrest Schrems II van het Hof, punt 192.

²² Arrest Schrems II van het Hof, punt 195.

²³ Ontwerpbesluit, bijlage I, hoofdstuk I, laatste zin.

onder meer rekening houden met de internationale toezeggingen die het derde land heeft gedaan, of andere verplichtingen die voortvloeien uit de deelname van dat derde land aan multilaterale of regionale regelingen, in het bijzonder met betrekking tot de bescherming van persoonsgegevens, alsook met de nakoming van deze verplichtingen.

23. De VS zijn partij bij verschillende internationale overeenkomsten die het recht op privacy waarborgen, zoals het Internationaal Verdrag inzake burgerrechten en politieke rechten (artikel 17), het Verdrag inzake de rechten van personen met een handicap (artikel 22) en het Verdrag inzake de rechten van het kind (artikel 16). Voorts houden de VS zich als OESO-lid aan het privacykader van de OESO, met name de richtsnoeren voor de bescherming van de privacy en de grensoverschrijdende stromen van persoonsgegevens. Op 14 december 2022 hebben de ministers en hoge vertegenwoordigers van de OESO-leden en de Europese Unie de OESO-verklaring over overheidstoegang tot door particuliere instanties bijgehouden persoonsgegevens aangenomen. De VS zijn ook partij bij het Verdrag van Boedapest inzake cybercriminaliteit.
24. Daarnaast zijn de VS lid van het systeem van grensoverschrijdende privacyregels (Cross-Border Privacy Rules, “CBPR”) van de economische samenwerking Azië-Stille Oceaan (APEC), een door de overheid gesteunde certificering van gegevensbescherming waartoe bedrijven kunnen toetreden om aan te tonen dat zij de internationaal erkende privacyregels naleven. Deze privacyregels zijn bekrachtigd door de leiders van de APEC.
25. Het EDPB neemt tevens kennis van de deelname van de VS als waarnemende staat aan de werkzaamheden van het Raadgevend Comité van Verdrag nr. 108 van de Raad van Europa.
26. Voorts neemt het EDPB kennis van en is hij ingenomen met de voortdurende betrokkenheid van VS-organen bij de in 2021 opgerichte “Rondetafel van gegevensbeschermings- en privacyautoriteiten van de G7” (G7 DPA Roundtable), waarin onafhankelijke toezichthoudende autoriteiten voor gegevensbescherming en privacy van de G7-landen bijeenkomen. In dit verband hebben zij bijvoorbeeld het recentste communiqué van de G7 DPA Roundtable²⁴ gesteund dat op 8 september 2022 in Bonn, Duitsland, is aangenomen en waarin het concept “Data Free Flow with Trust” (“vrije gegevensstroom met vertrouwen”) centraal stond.

1.3.3 Vooruitgang op het gebied van wetgeving inzake gegevensbescherming in de VS

27. Het EDPB neemt met name kennis van de ontwikkelingen op het gebied van wetgeving inzake gegevensbescherming op het niveau van de Amerikaanse staten. Het EDPB verwelkomt de vaststelling van wetgeving inzake gegevensbescherming die in vijf staten (Californië, Colorado, Connecticut, Virginia en Utah) in werking is getreden of tegen 2023 in werking zal treden²⁵.

²⁴ Rondetafel van de gegevensbeschermings- en privacyautoriteiten van de G7, “Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces” (“Bevordering van de vrije gegevensstroom met vertrouwen en kennisuitwisseling over de vooruitzichten voor internationale gegevensruimten”), 8 september 2022, https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1

²⁵ California Consumer Privacy Act (wet van Californië op de consumentenprivacy) (2018; van kracht sinds 1 januari 2020); California Privacy Rights Act (wet van Californië op de privacyrechten) (2020; volledig van kracht sinds 1 januari 2023); Colorado Privacy Act (wet van Colorado op de privacyrechten) (2021; van kracht sinds 1 juli 2023); Connecticut Data Privacy Act (wet van Connecticut op de gegevensbescherming) (2022; van kracht sinds 1 juli 2023); Virginia Consumer Data Protection Act (wet van Virginia op de bescherming van consumentengegevens) (2021; van kracht sinds 1 januari 2023); Utah Consumer Privacy Act (wet van Utah op de consumentenprivacy) (2022; van kracht op 31 december 2023).

28. Het EDPB merkt tevens op dat in vele andere staten van de VS reeds overeenkomstige initiatieven voor verdere wetgeving zijn genomen.
29. Voorts verwelkomt het EDPB uitdrukkelijk de inspanningen met betrekking tot het tweepartijdige initiatief voor een federale wet inzake gegevensbescherming, de American Data Privacy and Protection Act (ADPPA, Amerikaanse wet op de privacy en bescherming van gegevens).

1.3.4 Toepassingsgebied van het ontwerpbesluit

30. Volgens artikel 1 van het ontwerpbesluit concludeert de Commissie dat de VS een passend beschermingsniveau waarborgen voor persoonsgegevens die vanuit de EU worden doorgegeven aan organisaties in de Verenigde Staten die zijn opgenomen in de lijst van het kader voor gegevensbescherming ("Data Privacy Framework List"), die door het Amerikaanse ministerie van Handel wordt bijgehouden en openbaar gemaakt, overeenkomstig hoofdstuk I, punt 3 van bijlage I²⁶.
31. Het DPF is beschikbaar voor bedrijven die onder de jurisdictie van de FTC of het Amerikaanse ministerie van Vervoer vallen. Er wordt op gewezen dat in de toekomst andere Amerikaanse overheidsinstanties met soortgelijke bevoegdheden kunnen worden toegevoegd²⁷.

1.3.5 Beperkingen op de verplichting tot naleving van de DPF-beginselen

32. In bijlage I, hoofdstuk I, punt 5, is bepaald dat de naleving van de DPF-beginselen door DPF-organisaties onder meer kan worden beperkt i) voor zover nodig om te voldoen aan een rechterlijk bevel of aan vereisten van algemeen belang, rechtshandhaving²⁸ of nationale veiligheid²⁹ (ook wanneer wetten of overheidsreglementering tegenstrijdige verplichtingen scheppen) en ii) op grond van een wet, rechterlijk bevel of overheidsvoorschrift die/dat uitdrukkelijke bevoegdheden schept, op voorwaarde dat een DPF-organisatie bij de uitoefening van een dergelijke bevoegdheid kan aantonen dat haar niet-naleving van de DPF-beginselen beperkt blijft tot de mate die nodig is om te voldoen aan de dwingende rechtmatige belangen die met die bevoegdheid worden bevorderd.
33. Zonder volledige kennis van de Amerikaanse wetgeving op zowel federaal niveau als op het niveau van de staten is het voor het EDPB moeilijk om de reikwijdte van de in dit lid opgesomde vrijstellingen in detail te beoordelen. Daarom beveelt het EDPB aan dat de Commissie in het ontwerpbesluit een verduidelijking opneemt van de reikwijdte van de vrijstellingen, met inbegrip van de toepasselijke waarborgen krachtens het Amerikaanse recht, teneinde de gevolgen van deze vrijstellingen voor het beschermingsniveau van de betrokkenen beter te kunnen bepalen. Het EDPB onderstreept tevens dat de Commissie op de hoogte moet worden gebracht van en toezicht moet houden op de toepassing en vaststelling van elke wet die of elk overheidsvoorschrift dat gevolgen heeft voor de naleving van de DPF-beginselen.

²⁶ Ontwerpbesluit, slotoverwegingen, artikel 1, blz. 57 (in de Engelstalige versie). Het EDPB begrijpt dat het ontwerpbesluit geen betrekking zal hebben op doorgiften aan gecertificeerde entiteiten in de VS door buiten de EU gevestigde entiteiten die krachtens artikel 3, lid 2, AVG, aan de AVG onderworpen zijn.

²⁷ Ontwerpbesluit, bijlage I, hoofdstuk I, punt 2.

²⁸ Zie punt 3.1 van dit advies voor meer opmerkingen over het gebruik van onder het EU-VS-DPF vallende persoonsgegevens voor rechtshandavingsdoeleinden.

²⁹ Zie punt 3.2 van dit advies voor meer opmerkingen over het gebruik van onder het EU-VS-DPF vallende persoonsgegevens voor doeleinden van nationale veiligheid.

1.3.6 Wijzigingen met betrekking tot het “privacyschild”

34. Het EDPB is ingenomen met de inspanningen die zijn geleverd om de vereisten van het arrest Schrems II aan te pakken. Niettemin zou het EDPB het hebben toegejuicht indien bij de onderhandelingen over het DPF ook aandacht zou zijn besteed aan meer kwesties die i) in Advies 01/2016 van de Groep gegevensbescherming artikel 29 en ii) in de eerdere gezamenlijke evaluaties³⁰ aan de orde zijn gesteld.
35. Het EDPB merkt ook op dat, ondanks een aantal wijzigingen en aanvullende toelichtingen in de overwegingen van het ontwerpbesluit, de DPF-beginselen waaraan de DPF-organisaties zich moeten houden in wezen ongewijzigd blijven ten opzichte van die welke van toepassing zijn in het kader van het privacyschild.

1.3.7 Gebrek aan duidelijkheid in de documenten van het DPF

36. Het EDPB merkt op dat door de structuur en de nummering van de bijlagen de informatie nogal moeilijk te vinden en te raadplegen valt. Dit draagt bij tot een algemene complexe presentatie van het nieuwe kader, met in de bijlagen een verzameling documenten van verschillende juridische waarde, en is wellicht niet bevorderlijk voor een goed begrip van de DPF-beginselen door betrokkenen, DPF-organisaties en gegevensbeschermingsautoriteiten van de EU (“EU-DPA’s”).
37. Het EDPB benadrukt tevens dat de terminologie in het gehele DPF consistent moet worden gebruikt. Dit is momenteel bijvoorbeeld niet het geval voor het begrip “verwerking”. In sommige delen van het DPF worden namelijk bepaalde soorten gegevensverwerkingsactiviteiten opgesomd en wordt de term “verwerking” niet gebruikt. Dit kan leiden tot rechtsonzekerheid en mogelijke lacunes in de bescherming³¹.
38. Het EDPB verheugt zich erover dat definities van sommige van de gebruikte termen in het DPF zijn opgenomen³². Dit is echter niet het geval voor sommige andere essentiële termen, zoals ten minste “vertegenwoordiger” of “verwerker”, die volgens het EDPB een duidelijke en specifieke definitie verdienen in bijlage I, hoofdstuk I, punt 8, van het DPF, en een definitie waarover zowel de VS als de EU het eens zijn, om verwarring in een later stadium te voorkomen voor DPF-organisaties die zich op het DPF beroepen, de toezichthoudende autoriteiten en het grote publiek.

³⁰ Jaarlijkse evaluaties: EU-VS-privacyschild — eerste jaarlijkse gezamenlijke evaluatie, WP 255, verslag van de Groep gegevensbescherming artikel 29 vastgesteld op 28 november 2017 (hierna het “eerste jaarlijkse gezamenlijke evaluatieverslag” genoemd); EU-VS-privacyschild — tweede jaarlijkse gezamenlijke evaluatie, EDPB-verslag vastgesteld op 22 januari 2019 (hierna het “tweede jaarlijkse gezamenlijke evaluatieverslag” genoemd); EU-VS-privacyschild — derde jaarlijkse gezamenlijke evaluatie, EDPB-verslag vastgesteld op 12 november 2019 (hierna het “derde jaarlijkse gezamenlijke evaluatieverslag” genoemd).

³¹ Bijvoorbeeld: i) volgens de formulering van het ontwerpbesluit, bijlage I, hoofdstuk III, punt 6, f), zouden de DPF-beginselen alleen van toepassing zijn wanneer de organisatie de ontvangen gegevens “opslaat, gebruikt of openbaar maakt” (d.w.z. niet voor andere handelingen die onder het begrip “verwerking” vallen, zoals verzamelen, vastleggen, wijzigen, opvragen, raadplegen, wissen) en ii) volgens het ontwerpbesluit, bijlage I, hoofdstuk II, punt 4, a), zou gegevensbeveiliging alleen worden opgelegd voor het “creëren, bijhouden, gebruiken of verspreiden” van persoonsgegevens.

³² Ontwerpbesluit, bijlage I, hoofdstuk I, punt 8.

39. Wat betreft de kwestie van de uiteenlopende interpretaties in de EU en de VS van het begrip personeelsgegevens, is het EDPB het eens met het derde evaluatieverslag van de Commissie over de doelstelling om de besprekingen met de Amerikaanse autoriteiten voort te zetten³³.

2 ALGEMENE ASPECTEN VAN GEGEVENSBESCHERMING

2.1 Inhoudelijke beginselen

2.1.1 Begrippen

40. Op basis van de AVG-adequaateitsreferentie moeten er in het rechtskader van het derde land basisbegrippen en/of -beginselen inzake gegevensbescherming bestaan. Hoewel deze geen kopie hoeven te zijn van de terminologie die in de AVG wordt gehanteerd, moeten zij wel een afspiegeling vormen van de begrippen in de Europese wetgeving inzake gegevensbescherming en daarmee consistent zijn. In de AVG zijn bijvoorbeeld de volgende belangrijke begrippen opgenomen: “persoonsgegevens”, “verwerking van persoonsgegevens”, “verwerkingsverantwoordelijke”, “verwerker”, “ontvanger” en “gevoelige gegevens”. Het EDPB is verheugd dat definities van de termen “persoonsgegevens”, “verwerking” en “verwerkingsverantwoordelijke” in het DPF zijn opgenomen, zoals dat ook het geval was in het privacychild.
41. Het EDPB merkt op dat het onduidelijk blijft in hoeverre de DPF-beginselen van toepassing zijn op DPF-organisaties die persoonsgegevens uit de EU ontvangen voor “louter verwerkingsdoeleinden” (aangeduid als “vertegenwoordigers” of “verwerkers”). In het DPF wordt geen onderscheid gemaakt tussen DPF-beginselen die van toepassing zijn op vertegenwoordigers en DPF-beginselen die van toepassing zijn op verwerkingsverantwoordelijken, terwijl verscheidene van de in de DPF-beginselen opgenomen verplichtingen niet geschikt zijn voor vertegenwoordigers/verwerkers. Zo kan een vertegenwoordiger/verwerker natuurlijke personen niet alle elementen van de volledige kennisgeving verstrekken zoals vereist door het kennisgevingsbeginsel (bijvoorbeeld de doeleinden waarvoor hij persoonsgegevens over hen verzamelt en gebruikt)³⁴, aangezien een vertegenwoordiger/verwerker niet op zijn eentje de middelen en doeleinden van de verwerking kan bepalen³⁵.

2.1.2 Het beginsel van doelbinding

42. In de AVG-adequaateitsreferentie is, in overeenstemming met de AVG, bepaald dat persoonsgegevens voor een specifiek doel moeten worden verwerkt en vervolgens alleen mogen worden gebruikt voor zover dit niet onverenigbaar is met het doel van de verwerking.
43. Het beginsel van gegevensintegriteit en doelbinding bepaalt dat een organisatie geen persoonlijke informatie mag verwerken op een wijze die onverenigbaar is met de doeleinden waarvoor deze is verzameld of waarmee de betrokkene achteraf heeft ingestemd³⁶. Het EDPB merkt op dat bij de beginselen van kennisgeving, keuze en gegevensintegriteit en doelbinding verschillende terminologie

³³ Derde jaarlijkse gezamenlijke evaluatieverslag, blz. 5, 15, 16 en 30; zie ook het werkdocument van de diensten van de Commissie bij het verslag van de Commissie aan het Europees Parlement en de Raad over de derde jaarlijkse evaluatie van de werking van het EU-VS-privacychild, blz. 17-18.

³⁴ Ontwerpbesluit, bijlage I, hoofdstuk II, punt 1, a).

³⁵ Zie ook Advies 01/2016 van de Groep gegevensbescherming artikel 29, blz. 16.

³⁶ Ontwerpbesluit, bijlage I, hoofdstuk II, punt 5.

wordt gebruikt. Zoals opgemerkt door de Groep gegevensbescherming artikel 29 en ondanks een nuttige verduidelijking in de overwegingen van het ontwerpbesluit, worden in het DPF termen als “verschillende doeleinden”, “wezenlijk verschillende” doeleinden of “een gebruik dat niet in overeenstemming is met” gebruikt zonder dat deze begrippen daarin duidelijk worden gedefinieerd, wat tot rechtsonzekerheid kan leiden.

2.1.3 Recht van inzage, rectificatie, wissing en bezwaar

44. In het DPF wordt het recht van betrokkenen op toegang, rectificatie en wissing geregeld door het toegangsbeginnsel³⁷.
45. Het toegangsbeginnsel zoals dat in het privacyschild was opgenomen, blijft ongewijzigd. Bijgevolg zijn sommige punten van zorg die in Advies 01/2016 van de Groep gegevensbescherming artikel 29 werden geformuleerd, nog steeds geldig, zoals hieronder wordt uiteengezet.
46. Met betrekking tot het recht op toegang van natuurlijke personen vindt het EDPB het nodig te herhalen dat de details van de verplichting om verzoeken van natuurlijke personen te beantwoorden beter in de hoofdtekst van het beginnsel kunnen worden opgenomen (ze worden nu alleen nog in een voetnoot beschreven³⁸). Ook moet duidelijk zijn dat toegang moet worden verleend voor zover een DPF-organisatie persoonsgegevens verwerkt, en niet alleen wanneer zij deze “opslaat”³⁹. Volgens het EDPB zou de huidige formulering kunnen leiden tot een enge interpretatie van het recht op toegang.
47. Wat de lijst van uitzonderingen op het recht van toegang betreft⁴⁰, neigen sommige nog steeds naar een verschuiving in de richting van de belangen van de DPF-organisaties. Het blijft het EDPB zorgen baren dat er in die gevallen geen verplichting lijkt te bestaan om rekening te houden met de rechten en belangen van de betrokkene⁴¹.
48. Een andere uitzondering, waarover de Groep gegevensbescherming artikel 29 zich al eerder zorgen heeft gemaakt⁴² en die het EDPB te ruim lijkt, is de uitzondering op het toegangsrecht voor informatie die voor het publiek toegankelijk is en informatie uit openbare documenten⁴³. Het EDPB heeft herhaaldelijk verklaard dat betrokkenen volgens het EU-recht altijd recht hebben op toegang tot hun gegevens, ongeacht of de persoonsgegevens al dan niet openbaar zijn gemaakt. Indien verzoeken om toegang zouden worden afgewezen op grond van het feit dat de gegevens zijn verkregen uit openbare bronnen of uit openbare documenten, zouden de betrokkenen de mogelijkheid verliezen om de juistheid van de gegevens te controleren en om te controleren of de gegevens überhaupt rechtmatig openbaar zijn gemaakt.
49. Het EDPB herinnert eraan dat het recht van toegang is vastgelegd in artikel 8, lid 2, van het Handvest. Hoewel dit geen absoluut recht is, is het fundamenteel voor het recht op bescherming van persoonsgegevens omdat het de uitoefening van de andere rechten van de betrokkene, zoals correctie en wissing, en het recht om bezwaar te maken, vergemakkelijkt⁴⁴.

³⁷ Ontwerpbesluit, bijlage I, hoofdstuk II, punt 6 en hoofdstuk III, punt 8, a), i).

³⁸ Ontwerpbesluit, bijlage I, hoofdstuk III, punt 8, a), i), 1) — voetnoot 14.

³⁹ Ontwerpbesluit, bijlage I, hoofdstuk III, punt 8, d), ii).

⁴⁰ Ontwerpbesluit, bijlage I, hoofdstuk III, punt 8, e).

⁴¹ Advies 01/2016 van de Groep gegevensbescherming artikel 29, punt 2.2.5.

⁴² Advies 01/2016 van de Groep gegevensbescherming artikel 29, punt 2.2.9.

⁴³ Ontwerpbesluit, bijlage I, hoofdstuk III, punt 15, d) en e).

⁴⁴ Advies 01/2016 van de Groep gegevensbescherming artikel 29, punt 2.2.5.

50. Naast het recht van toegang, het recht op wissing en het recht op schrapping heeft de betrokkene ook te allen tijde het recht om, op dwingende gerechtvaardigde gronden die verband houden met zijn/haar specifieke situatie, bezwaar te maken tegen de verwerking van zijn/haar gegevens onder bepaalde voorwaarden die zijn vastgelegd in het rechtskader van het derde land⁴⁵.
51. Met het keuzebeginsel voorziet het DPV in een recht om bezwaar te maken (opt-out) tegen de verstrekking van persoonsgegevens aan derden of tegen het gebruik van persoonsgegevens voor een wezenlijk verschillend doel⁴⁶. Bovendien hebben natuurlijke personen te allen tijde het recht zich te verzetten tegen het gebruik van hun persoonsgegevens voor direct-marketingdoeleinden⁴⁷. Behalve in het kader van direct marketing zijn de modaliteiten, met name het tijdschema, voor de uitoefening van het recht om bezwaar te maken, niet gedetailleerd vermeld. Daarom verzoekt het EDPB de Commissie te verduidelijken hoe natuurlijke personen hun recht om bezwaar te maken, kunnen uitoefenen.
52. Zoals gesteld in Advies 01/2016 van de Groep gegevensbescherming artikel 29, is het EDPB van mening dat de loutere verwijzing naar het bestaan van dit recht in het privacybeleid niet kan volstaan. Een geïndividualiseerde mogelijkheid om dit recht uit te oefenen moet niet alleen worden geboden in geval van openbaarmaking of hergebruik van persoonsgegevens. Het EDPB benadrukt dat in het DPV een algemeen recht moet worden geboden om bezwaar te maken op dwingende rechtmatige gronden in verband met de bijzondere situatie van de betrokkene. Het EDPB beveelt aan dat dit recht om bezwaar te maken op elk moment wordt gewaarborgd, en dat dit recht niet beperkt blijft tot het gebruik van de gegevens voor direct marketing⁴⁸.
53. Met betrekking tot personeelsgegevens waardeert het EDPB de verduidelijkingen van de Commissie wat betreft de toepassing van het kennisgevingsbeginsel en het keuzebeginsel wanneer een gecertificeerde Amerikaanse organisatie voornemens is personeelsgegevens te gebruiken voor een ander, niet-werkgerelateerd doel, zoals marketingcommunicatie⁴⁹. Het EDPB blijft er echter bij dat verdere verwerking van personeelsgegevens voor niet-werkgerelateerde doeleinden in de meeste gevallen als onverenigbaar met het oorspronkelijke doel zal worden beschouwd, en dat toestemming zelden volledig vrij zal zijn wanneer zij in een werkgerelateerd kader wordt gegeven.
54. Het EDPB herhaalt ook de bezwaren van de Groep gegevensbescherming artikel 29 met betrekking tot de uitzondering op het kennisgevingsbeginsel en het keuzebeginsel voor personeelsgegevens voor zover en voor zolang dat nodig is om te voorkomen dat afbreuk wordt gedaan aan het vermogen van de organisatie om bevorderingen, benoemingen of andere soortgelijke beslissingen over werk te nemen⁵⁰, die het EDPB ruim en vaag vindt⁵¹.

2.1.4 Beperkingen ten aanzien van verdere doorgifte

55. Verdere doorgifte van de persoonsgegevens door de eerste ontvanger van de oorspronkelijke gegevensdoorgifte mag alleen worden toegestaan wanneer de latere ontvanger (dat wil zeggen de ontvanger van de verdere doorgifte) eveneens is onderworpen aan voorschriften (met inbegrip van contractuele bepalingen) die een passend beschermingsniveau opleveren en deze ontvanger de

⁴⁵ AVG-a-dequa-atheidsreferentie, hoofdstuk 3, punt A, 8).

⁴⁶ Ontwerpbesluit, bijlage I, hoofdstuk II, punt 2, a).

⁴⁷ Ontwerpbesluit, bijlage I, hoofdstuk III, punt 12, a).

⁴⁸ Advies 01/2016 van de Groep gegevensbescherming artikel 29, punt 2.2.2.

⁴⁹ Ontwerpbesluit, bijlage I, hoofdstuk III, punt 9, b), i) en overweging 15 en voetnoot 27.

⁵⁰ Ontwerpbesluit, bijlage I, hoofdstuk III, punt 9, b), iv).

⁵¹ Advies 01/2016 van de Groep gegevensbescherming artikel 29, punt 2.2.7.

relevante instructies opvolgt wanneer hij/zij namens de verwerkingsverantwoordelijke gegevens verwerkt. Het beschermingsniveau van natuurlijke personen wier gegevens worden doorgegeven, mag niet worden ondermijnd door de verdere doorgifte. De eerste ontvanger van de gegevens die vanuit de EU worden doorgegeven, heeft de verantwoordelijkheid om bij ontstentenis van een adequaatheidsbesluit toe te zien op passende waarborgen voor verdere doorgifte van gegevens. Verdere doorgiften van gegevens mogen alleen plaatsvinden voor beperkte en welbepaalde doeleinden en voor zover er een rechtsgrondslag voor de verwerking is⁵².

56. Volgens het verantwoordingsbeginsel voor verdere doorgiften in het DPF kan verdere doorgifte alleen plaatsvinden voor beperkte en gespecificeerde doeleinden, op basis van een overeenkomst tussen de DPF-organisatie en de derde (of een vergelijkbare regeling binnen een concern) en alleen als die overeenkomst de derde verplicht hetzelfde beschermingsniveau te bieden als het niveau dat door de DPF-beginselen wordt gewaarborgd⁵³.
57. Het EDPB herhaalt de in Advies 01/2016 van de Groep gegevensbescherming artikel 29 geuite bezorgdheid over de vrijstelling van de noodzaak van een contract voor doorgiften binnen een groep tussen verwerkingsverantwoordelijken⁵⁴. Met betrekking tot personeelsgegevens begrijpt het EDPB nog steeds niet de reden voor de vrijstelling van de verplichting om een contract te sluiten met een derde verwerkingsverantwoordelijke in geval van verdere doorgifte voor “incidentele werkgerelateerde operationele behoeften”⁵⁵.
58. Voorts wenst het EDPB het verzoek van de Groep gegevensbescherming artikel 29⁵⁶ te herhalen dat door het kader gebonden organisaties vóór een verdere doorgifte moeten beoordelen of de dwingende vereisten van de nationale wetgeving van het derde land die van toepassing is op de ontvanger, de continuïteit van de bescherming van de betrokkenen wier gegevens worden doorgegeven, niet zouden ondermijnen⁵⁷.
59. Het EDPB stelt dat de verdere doorgifte van persoonsgegevens aan derde landen kan leiden tot inbreuken op de grondrechten van natuurlijke personen en verzoekt de Commissie te verduidelijken dat de waarborgen die door de eerste ontvanger aan de importeur in het derde land worden opgelegd

⁵² AVG-adequaateitsreferentie, hoofdstuk 3, punt A, 9).

⁵³ Ontwerpbesluit, bijlage I, II.3.

⁵⁴ Ontwerpbesluit, bijlage I, hoofdstuk III, punt 10, b), i), waarin wordt verwezen naar “of andere instrumenten binnen een groep (bv. nalevings- en controleprogramma’s)” die blijkbaar niet bindend hoeven te zijn.

⁵⁵ Ontwerpbesluit, bijlage I, hoofdstuk III, punt 9, e), i), waarin wordt verwezen naar voorbeelden zoals verzekeringsdekking.

⁵⁶ Advies 01/2016 van de Groep gegevensbescherming artikel 29, punt 2.2.3, blz. 21.

⁵⁷ [In het licht van het arrest Schrems II heeft het EDPB in een aantal richtsnoeren en aanbevelingen de verplichtingen voor exporteurs en importeurs van gegevens met betrekking tot verdere doorgiften verder verduidelijkt: zie Aanbevelingen 01/2020 van het EDBP inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen \(Versie 2.0, vastgesteld op 18 juni 2021\); Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen \(Vastgesteld op 10 november 2020\); Richtsnoeren 04/2021 voor gedragscodes als instrumenten voor doorgifte, \(Versie 2.0, vastgesteld op 22 februari 2022\); Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules \(Aanbevelingen 1/2022 over het verzoek om goedkeuring en over de elementen en beginselen die in bindende bedrijfsvoorschriften voor de verwerkingsverantwoordelijke moeten worden opgenomen, vastgesteld op 14 november 2022\); Guidelines 07/2022 on certification as a tool for transfers \(Richtsnoeren 07/2022 betreffende certificering als instrument voor doorgiften, vastgesteld na openbare raadpleging op 14 februari 2023\).](#)

doeltreffend moeten zijn in het licht van de wetgeving van het derde land voordat een verdere doorgifte in het kader van het DPF plaatsvindt⁵⁸.

2.1.5 Geautomatiseerde besluitvorming en profilering

60. Besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking (geautomatiseerde individuele besluitvorming), waaronder profilering, waaraan voor de betrokkene 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. Voorbeelden van zulke voorwaarden in het Europees rechtskader zijn dat de uitdrukkelijke toestemming van de betrokkene moet worden verkregen of dat de doorgifte noodzakelijk is voor de sluiting van een overeenkomst. Als het besluit niet voldoet aan de voorwaarden die in het rechtskader van het derde land zijn neergelegd, moet de betrokkene het recht hebben er niet aan te worden onderworpen. De wetgeving van het derde land moet in elk geval voorzien in de noodzakelijke waarborgen, waaronder het recht te worden geïnformeerd over specifieke redenen die ten grondslag liggen aan het besluit en de onderliggende logica, onjuiste of onvolledige informatie te corrigeren en het besluit aan te vechten wanneer dit is goedgekeurd op basis van onjuiste gegevens⁵⁹.
61. Het DPF voorziet niet in specifieke wettelijke waarborgen wanneer natuurlijke personen worden onderworpen aan besluiten waaraan voor hen rechtsgevolgen zijn verbonden of die hen in aanmerkelijke mate treffen en die louter wordt genomen op grond van een geautomatiseerde gegevensverwerking die bestemd is om bepaalde aspecten van hun persoonlijkheid, zoals beroepsprestatie, kredietwaardigheid, betrouwbaarheid, gedrag, enz. te evalueren.
62. Zoals reeds in Advies 01/2016 van de Groep gegevensbescherming artikel 29 en door het EDPB in zijn eerdere adviezen over de adequaatheidsbesluiten met betrekking tot Japan en Zuid-Korea⁶⁰ is overwogen, stelt het EDPB vast dat de snelle ontwikkelingen op het gebied van geautomatiseerde besluitvorming en profilering — in toenemende mate door middel van AI-technologieën — in dit verband bijzondere aandacht vergen⁶¹.
63. Het EDPB neemt kennis van de argumenten van de Commissie volgens welke het ontbreken van specifieke regels inzake geautomatiseerde besluitvorming in het DPF waarschijnlijk geen invloed zal hebben op het beschermingsniveau met betrekking tot persoonsgegevens die in de Unie zijn verzameld (aangezien elk besluit op basis van geautomatiseerde verwerking normaliter wordt genomen door de verwerkingsverantwoordelijke in de Unie die een directe relatie met de betrokkene heeft)⁶². Volgens het EDPB kan echter niet worden uitgesloten dat een in de VS gevestigde verwerkingsverantwoordelijke geautomatiseerde besluitvorming toepast op gegevens die krachtens het ontwerpbesluit worden doorgegeven (bijvoorbeeld in het kader van werk, voor de beoordeling van prestaties op het werk, verzekeringen, huisvesting).

⁵⁸ Advies 01/2016 van de Groep gegevensbescherming artikel 29, punt 2.2.3, blz. 21.

⁵⁹ AVG-adequaateisreferentie, hoofdstuk 3, punt B, 3).

⁶⁰ [Advies 28/2018 van het EDPB over het ontwerpuitvoeringsbesluit van de Europese Commissie betreffende de adequate bescherming van persoonsgegevens in Japan, goedgekeurd op 5 december 2018](#); [Advies 32/2021 van het EDPB over het ontwerpuitvoeringsbesluit van de Europese Commissie betreffende de passende bescherming van persoonsgegevens in de Republiek Korea, goedgekeurd op 24 september 2021](#).

⁶¹ Zie onder andere C-634/21, OQ/Land Hessen (SCHUFA Holding e.a.), verzoek om een prejudiciële beslissing (hangende).

⁶² Ontwerpbesluit, overwegingen 33 en 34.

64. Het EDPB is ingenomen met de verwijzingen van de Commissie naar specifieke waarborgen waarin de desbetreffende Amerikaanse wetgeving op verschillende gebieden voorziet⁶³. Volgens het EDPB lijkt het beschermingsniveau voor natuurlijke personen echter te variëren naargelang van de eventuele sectorspecifieke regels die op de betrokken situatie van toepassing zijn. Het risico bestaat dat sommige situaties niet worden gedekt omdat zij niet binnen de werkingssfeer van de genoemde rechtshandelingen vallen. Voorts wordt de inhoud van de individuele rechten in verband met geautomatiseerde besluitvorming in de verschillende rechtshandelingen verschillend beschreven.
65. Tegen deze achtergrond is het EDPB van oordeel dat in de DPF specifieke regels betreffende geautomatiseerde besluitvorming nodig zijn om voldoende waarborgen te bieden, waaronder het recht van de betrokkene om de betrokken logica te kennen, het besluit aan te vechten en menselijke tussenkomst te verkrijgen wanneer het besluit hem of haar in aanzienlijke mate treft⁶⁴.

2.2 Procedurele en handhavingsmechanismen

66. Het EDPB merkt op dat het DPF blijft uitgaan van een systeem van zelfcertificering, ook al noemt de Commissie het een systeem van “certificering”.
67. Het EDPB herinnert aan de verbeteringen die in de loop van de vorige gezamenlijke evaluaties zijn bereikt. Bijvoorbeeld wat betreft de rol van het ministerie van Handel, het (her)zelfcertificeringsproces (...), het toezicht op de naleving van de DPF-beginselen door bedrijven (bv. door steekproefsgewijze controles, het gebruik van nalevingsvragenlijsten) en het opsporen en aanpakken van valse beweringen aangaande deelname (bv. door opzoeken op internet).
68. Tegelijkertijd hadden de Groep gegevensbescherming artikel 29 en het EDPB hun bezorgdheid geuit over een zeker gebrek aan toezicht op de naleving van de vereisten van het privacyschild⁶⁵. Het EDPB is het met name eens met de bevindingen van de Commissie na de derde jaarlijkse evaluatie van het privacyschild dat de steekproefsgewijze controles door het ministerie van Handel in het kader van het privacyschild meestal beperkt blijven tot vormvereisten (zoals niet-reagerende contactpunten of het niet online toegankelijk zijn van het privacybeleid van een onderneming)⁶⁶. Het EDPB is van mening dat nalevingscontroles met betrekking tot meer materiële vereisten cruciaal zijn.
69. Het EDPB herinnert ook aan het belang van doeltreffend toezicht (ook op de naleving van materiële vereisten) en handhaving van het DPF. Dit aspect zal door het EDPB nauwlettend worden gevolgd, onder meer in het kader van de periodieke evaluaties.
70. Wat de handhaving betreft, neemt het EDPB kennis van de hernieuwde toezeggingen in de brieven van de FTC⁶⁷ en het Amerikaanse ministerie van Vervoer⁶⁸ om prioriteit te geven aan het onderzoek van vermeende schendingen van het DPF, passende handhavingsmaatregelen te nemen tegen entiteiten die valse of misleidende beweringen aangaande deelname doen, toe te zien op handhavingsbevelen betreffende schendingen van het DPF en samen te werken met de gegevensbeschermingsautoriteiten van de EU. In dit verband erkent het EDPB ook dat de FTC heeft

⁶³ Ontwerpbesluit, overweging 35.

⁶⁴ Zie ook derde jaarlijkse gezamenlijke evaluatieverslag, punt 76.

⁶⁵ Verslag over de derde jaarlijkse gezamenlijke evaluatie, punt 7.

⁶⁶ [Verslag van de Commissie aan het Europees Parlement en de Raad over de derde jaarlijkse evaluatie van de werking van het EU-VS-privacy Schild \(COM\(2019\)495 final van 23.10.2019\)](#), blz. 4.

⁶⁷ Ontwerpbesluit, bijlage IV.

⁶⁸ Ontwerpbesluit, bijlage V.

aangegeven dat zij voornemens is haar handhavingsinspanningen verder te richten op materiële schendingen van het DPF en dat zij voornemens is (ook) op eigen initiatief onderzoek te verrichten. Deze aspecten zullen door het EDPB nauwlettend worden gevolgd, ook in het kader van de periodieke evaluaties.

2.3 Verhaalmechanismen

71. Het EDPB is ingenomen met de duidelijke presentatie in het ontwerpbesluit van de zeven verhaalsmogelijkheden die aan de betrokkenen in de EU worden geboden indien hun persoonsgegevens in strijd met het DPF worden verwerkt⁶⁹.
72. Deze verschillende verhaalmechanismen zijn vastgesteld overeenkomstig de vereisten van het beginsel van verhaal, handhaving en aansprakelijkheid en het aanvullende beginsel 11 inzake “geschillenbeslechting en handhaving” van het ministerie van Handel, en worden vermeld in bijlage I bij het ontwerpbesluit⁷⁰.
73. Zoals de Commissie in haar ontwerpbesluit onderstreept, moet de betrokkene beschikken over effectieve mogelijkheden om administratief beroep of beroep in rechte in te stellen⁷¹. Dit sluit aan bij het vereiste van artikel 45, lid 2, punt a), AVG, volgens hetwelk de Commissie bij haar beoordeling van de vraag of het beschermingsniveau in een derde land adequaat is, met name rekening moet houden met “effectieve mogelijkheden om administratief beroep of beroep in rechte in te stellen voor betrokkenen wier persoonsgegevens worden doorgegeven”⁷². Aan dit vereiste wordt ook herinnerd in de AVG-adequaateitsreferentie⁷³.
74. Het EDPB merkt op dat deze verhaalmechanismen dezelfde zijn als die in het vroegere privacyschild, waarover de Groep gegevensbescherming artikel 29 opmerkingen had gemaakt⁷⁴.
75. Met betrekking tot het arbitragemechanisme merkt het EDPB op dat deze mogelijkheid niet beschikbaar is met betrekking tot de uitzonderingen op de DPF-beginselen⁷⁵ en verwijst daarom naar zijn opmerking in punt 33.
76. Met betrekking tot aanvullende rechtsmiddelen die in het Amerikaanse recht beschikbaar zijn, zou het EDPB ook graag nadere bijzonderheden over de genoemde wetgeving⁷⁶ ontvangen en verwijst hij naar zijn opmerking in punt 21.
77. Voorts is het EDPB ingenomen met de brief van de FTC waarin zij haar voornemen beschrijft om nauw samen te werken met de Europese gegevensbeschermingsautoriteiten⁷⁷. Het EDPB juicht ook toe dat de FTC prioriteit geeft aan klachten, hoewel dit de betrokkene misschien niet de zekerheid geeft dat zijn klachten in alle gevallen zullen worden behandeld.

⁶⁹ Ontwerpbesluit, overweging 67.

⁷⁰ Ontwerpbesluit, bijlage I, hoofdstuk II, punt 7, en hoofdstuk II, punt 11, en bijlage I bij bijlage I.

⁷¹ Ontwerpbesluit, overweging 64.

⁷² Zie ook overweging 141 van de AVG waarin wordt verwezen naar artikel 47 van het Handvest van de grondrechten voor het recht op een doeltreffende voorziening in rechte in de EU.

⁷³ AVG-adequaateitsreferentie, blz. 8.

⁷⁴ Zie met name Advies 01/2016 van de Groep gegevensbescherming artikel 29, punt 2.2.6, a).

⁷⁵ Ontwerpbesluit, bijlage I bij bijlage I, punt A.

⁷⁶ Ontwerpbesluit, overweging 85.

⁷⁷ Ontwerpbesluit, bijlage IV.

78. Wat betreft de mogelijkheid voor natuurlijke personen om in bepaalde gevallen hun klachten voor te leggen aan een Europese gegevensbeschermingsautoriteit, zou het EDPB graag nadere informatie ontvangen i) over de vraag of de mogelijkheid van de Europese gegevensbeschermingsautoriteit om advies te geven over corrigerende of compenserende maatregelen ook aanbevelingen voor boeten of het gebruik van onderzoeksbevoegdheden kan inhouden, en ii) over de vraag in hoeverre het optreden van de Europese gegevensbeschermingsautoriteit in aanmerking zou worden genomen als bewijs voor handhavingsmaatregelen door de FTC of het ministerie van Vervoer⁷⁸.
79. Het EDPB zal nauwlettend toezien op de doeltreffendheid van de verhaalmechanismen, ook in het kader van de periodieke evaluaties.

3 TOEGANG TOT PERSOONSgegevens DIE VANUIT DE EUROPESE UNIE WORDEN DOORgegeVEN EN HET GEBRUIK DAARVAN DOOR OVERHEIDSINSTANTIES IN DE VS

3.1 Toegang en gebruik met het oog op handhaving van het strafrecht

3.1.1 De toegang van rechtshandavingsinstanties tot persoonsgegevens moet gebaseerd zijn op duidelijke, nauwkeurige en toegankelijke regels

80. Het EDPB is ingenomen met de meer gedetailleerde informatie en toelichtingen, in vergelijking met het vorige adequaatheidsbesluit, die in het ontwerpbesluit zijn opgenomen met betrekking tot de toegang tot en het gebruik van persoonsgegevens door de Amerikaanse overheidsinstanties met het oog op handhaving van het strafrecht. Het ontwerpbesluit bevat in bijlage VI ook een brief van het Amerikaanse ministerie van Justitie, afdeling Strafrecht ("Criminal Division") met een kort overzicht van de primaire onderzoeksmiddelen die worden gebruikt om commerciële gegevens en andere opgeslagen gegevens van bedrijven in de Verenigde Staten te verkrijgen in het kader van strafrechtelijke vervolging of het openbaar belang (civiele en regelgevende doeleinden), waaronder de toegangsbeperkingen die zijn vastgesteld in deze bevoegdheden. Volgens de brief worden alle in de brief beschreven juridische procedures gebruikt om informatie te verkrijgen van bedrijven in de VS, ongeacht de nationaliteit of woonplaats van de betrokkene, en vloeien zij rechtstreeks voort uit de grondwet van de Verenigde Staten (het vierde amendement), uit de gewone wetten en het procesrecht of uit de richtsnoeren en de beleidsmaatregelen van het ministerie van Justitie. Dit overzicht heeft geen betrekking op de onderzoeksinstrumenten voor de nationale veiligheid die door de rechtshandavingsinstanties worden gebruikt bij onderzoeken naar terrorisme en andere onderzoeken in het kader van de nationale veiligheid⁷⁹.
81. Het EDPB merkt op dat het ontwerpbesluit en bijlage VI daarbij hoofdzakelijk betrekking hebben op federale rechtshandavings- en regelgevingsinstanties⁸⁰ en niet specifiek verwijzen naar de wetten van de staten die voorzien in deze procedures voor het verkrijgen van informatie. In bijlage VI wordt ook vermeld dat er andere juridische grondslagen bestaan voor bedrijven om verzoeken om gegevens van overheidsinstanties aan te vechten op basis van hun specifieke branche en de soorten gegevens die zij verwerken, waarbij bovendien verschillende, niet-uitputtende voorbeelden worden gegeven,

⁷⁸ Ontwerpbesluit, bijlage I, hoofdstuk III, punt 5, b), iii).

⁷⁹ Ontwerpbesluit, voetnoot 1 bij bijlage VI.

⁸⁰ Ontwerpbesluit, overwegingen 90 tot en met 93.

zoals de Bank Secrecy Act en de uitvoeringsbepalingen daarvan⁸¹, de Fair Credit Reporting Act⁸², de Right to Financial Privacy Act⁸³. Het EDPB merkt op dat de toepasselijke rechtsgrondslag voor een bepaald verzoek om toegang afhangt van de aard van de opgevraagde gegevens, de aard van het bedrijf, de aard van de juridische procedures (strafrechtelijk, administratief, in verband met andere openbare belangen) en de aard van de entiteit die om toegang verzoekt. Aangezien alle toepasselijke regels om de toegang van rechtshandavingsinstanties tot aan de VS overgedragen gegevens te beperken, gebaseerd zijn op de grondwet, op de gewone wetten en op transparant beleid van het ministerie van Justitie, erkent het EDPB de toegankelijkheid van deze regels en verzoekt het de Commissie dit element in het ontwerpbesluit tot uitdrukking te brengen. Volgens bijlage VI zijn deze gewone wetten van toepassing ongeacht de nationaliteit of de woonplaats van de betrokkene en omvatten zij in het algemeen de vereisten van het vierde amendement (hoewel zij vaak ook verder gaan en aanvullende bescherming bieden).

82. Concluderend neemt het EDPB kennis van de meer gedetailleerde beoordeling in het ontwerpbesluit in vergelijking met het vorige adequaatheidsbesluit wat betreft de toegang voor federale rechtshandavingsinstanties. Wat de toegang voor rechtshandavingsinstanties van de staten betreft, neemt het EDPB er ook kennis van dat volgens bijlage VI de bescherming van de wetgeving van de staten ten minste gelijk moet zijn aan die van de Amerikaanse grondwet, met inbegrip van maar niet beperkt tot het vierde amendement. Het EDPB verzoekt de Commissie het element van bescherming uit hoofde van de wetgeving van de staten bij toekomstige evaluaties nader te beoordelen.

3.1.2 De noodzakelijkheid en evenredigheid van de nagestreefde legitieme doelstellingen moeten worden aangetoond

83. Het EDPB neemt terdege nota van het feit dat verzoeken om toegang tot gegevens voor rechtshandavingsdoeleinden in het algemeen kunnen worden beschouwd als verzoeken met een legitieme doelstelling. Tegelijkertijd zijn dergelijke inmengingen echter alleen aanvaardbaar wanneer zij noodzakelijk en evenredig zijn⁸⁴.
84. Volgens vaste rechtspraak van het Hof vereist het evenredigheidsbeginsel dat de wettelijke maatregelen die een inmenging in het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens met zich meebrengen “geschikt zijn om de door de betrokken regeling nagestreefde legitieme doelstellingen te verwezenlijken en niet verder gaan dan wat daarvoor geschikt en noodzakelijk is”⁸⁵. Daarom vindt de beoordeling van de noodzakelijkheid en de

⁸¹ 31 U.S.C. § 5318; 31 C.F.R. Chapter X.

⁸² 15 U.S.C. § 1681b.

⁸³ 12 U.S.C. §§ 3401-3423.

⁸⁴ Zie het arrest van het Hof van Justitie van 6 oktober 2020 in de gevoegde zaken C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*, ECLI:EU:C:2020:791 (hierna “arrest *La Quadrature du Net* van het Hof” genoemd), punt 140. Zie ook [Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit](#) (Beoordeling van de noodzakelijkheid van maatregelen die het grondrecht op bescherming van persoonsgegevens beperken: een toolkit), EDPS, 11 april 2017 en [Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data](#) (Richtsnoeren voor de beoordeling van de evenredigheid van maatregelen die het grondrecht op privacy en op bescherming van persoonsgegevens beperken), EDPS, 19 december 2019.

⁸⁵ Zie het arrest van het Hof van Justitie van 8 april 2014 in de gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238 (hierna “arrest *Digital Rights Ireland* van het Hof” genoemd), punt 46 en de aldaar aangehaalde rechtspraak.

evenredigheid in beginsel altijd plaats met betrekking tot een specifieke, door de wetgeving beoogde maatregel.

85. De Amerikaanse autoriteiten specificeren in bijlage VI dat federale aanklagers en federale onderzoeksagenten in het kader van een strafrechtelijk onderzoek toegang kunnen krijgen tot documenten en andere gegevens van organisaties door middel van meerdere soorten dwingende juridische procedures, waaronder dagvaardingen van de kamer van inbeschuldigingstelling, administratieve dwangbevelen en huiszoekingsbevelen, op grond van federale bevoegdheden voor af luisteren en nummerregistratie⁸⁶. Instanties met civiele en regelgevende verantwoordelijkheden kunnen daarnaast een dagvaarding uitbrengen tegen een organisatie om bedrijfsgegevens, elektronisch opgeslagen informatie of andere tastbare zaken op te vragen⁸⁷. De procedures zelf worden ook toegelicht in de overwegingen 90 tot en met 93 van het ontwerpbesluit. Het EDPB wijst in dit verband op een positieve ontwikkeling in de Amerikaanse jurisprudentie betreffende elektronisch opgeslagen informatie, waarnaar in het ontwerpbesluit wordt verwezen⁸⁸.
86. In bijlage VI wordt voorts gespecificeerd dat deze juridische procedures niet-discriminerend zijn en in het algemeen worden gebruikt om informatie te verkrijgen van “ondernemingen” in de VS, ongeacht of zij al dan niet gecertificeerd zijn binnen het EU-VS-kader voor gegevensbescherming, en ongeacht de nationaliteit of woonplaats van de betrokkene.
87. Voorts bevat bijlage VI bevindingen betreffende de waarborgen uit hoofde van het vierde amendement van de grondwet van de Verenigde Staten, volgens welke voor huiszoekingen en inbeslagnemingen door rechtshandavingsinstanties in de eerste plaats een gerechtelijk bevel vereist is op grond van een bewijs van gereede aanleiding en een voldoende mate van gedetailleerdheid, en wordt in deze bijlage verwezen naar het feit dat de rechtshandavingsdiensten in uitzonderlijke gevallen waarin het bevel niet vereist is, onderworpen zijn aan een redelijkheidstoets uit hoofde van het vierde amendement⁸⁹. Een persoon die wordt onderworpen aan een zoeking of wiens eigendom wordt doorzocht, kan verzoeken om vernietiging van bewijs dat is verkregen of afgeleid van een onrechtmatige doorzoeking indien dat bewijs tijdens een strafproces tegen die persoon wordt ingebracht⁹⁰.
88. Concluderend merkt het EDPB op dat het systeem van onderzoeksinstrumenten dat wordt gebruikt om in de VS commerciële gegevens en andere opgeslagen gegevens van bedrijven te verkrijgen in het kader van strafrechtelijke vervolging of het openbaar belang — met inbegrip van de toegangsbeperkingen en waarborgen — een uitgebreid maar ook complex systeem van maatregelen vormt, dat onder meer het federale karakter van de Amerikaanse regering weerspiegelt.

⁸⁶ Ontwerpbesluit, bijlage VI, blz. 2.

⁸⁷ Ontwerpbesluit, bijlage VI, blz. 4.

⁸⁸ Ontwerpbesluit, voetnoot 146. In een arrest uit 2018 heeft het Hooggerechtshof van de Verenigde Staten bevestigd dat rechtshandavingsinstanties ook over een huiszoekingsbevel of een uitzonderlijke toelating tot huiszoeking zonder rechterlijk bevel moeten beschikken om toegang te krijgen tot historische locatiegegevens van mobiele telefoons, die een uitgebreid overzicht geven van de bewegingen van een gebruiker en dat de gebruiker een redelijke verwachting van privacy mag hebben met betrekking tot dergelijke informatie (Timothy Ivory Carpenter/United States of America, nr. 16-402, 585 U.S. (2018)).

⁸⁹ Ontwerpbesluit, bijlage VI, blz. 2.

⁹⁰ Ontwerpbesluit, overweging 90.

89. Derhalve kan worden gesteld dat het systeem van onderzoeksmaatregelen voor de rechtshandhaving in de VS in het algemeen voldoet aan de vereisten van noodzakelijkheid en evenredigheid met betrekking tot de grondrechten op eerbiediging van het privéleven en op gegevensbescherming.

3.1.3 Er moet een onafhankelijk toezichtmechanisme bestaan

90. Het EDPB neemt terdege nota van het feit dat voor de meeste procedures die in het ontwerpbesluit en in bijlage VI worden beschreven, een rechterlijke beslissing nodig is voordat de autoriteiten toegang krijgen tot gegevens (bv. rechterlijke bevelen voor “pen registers or trap and trace devices” (trackers van berichtenverkeer)⁹¹, rechterlijke bevelen voor toezicht op grond van de Federal Wiretap Law⁹², huiszoekingsbevelen – Federal Rules of Criminal Procedure, rule 41⁹³). Het lijkt er echter op dat niet voor al deze bevelen a priori de betrokkenheid van een rechter vereist is. Zo kunnen civiele en regelgevende instanties “dagvaardingen uitbrengen”⁹⁴. In deze gevallen bestaat echter de mogelijkheid van een rechterlijke toetsing achteraf van de redelijkheid van de dagvaarding, aangezien een ontvanger van een administratief dwangbevel de handhaving van dat dwangbevel kan aanvechten voor de rechter⁹⁵.
91. Voorts wordt in het ontwerpbesluit het toezicht op de federale rechtshandavingsinstanties door diverse organen beschreven, van de interne controle door de functionarissen voor privacy en burgerlijke vrijheden (Privacy and Civil Liberties Officers) tot de externe controle door de inspecteur-generaal (Inspector General) en specifieke commissies in het Amerikaanse Congres⁹⁶. De Europese Commissie verstrekt genuanceerde en gedetailleerde informatie en komt over het algemeen tot begrijpelijke conclusies. Het EDPB ziet er dan ook van af de feitelijke bevindingen en beoordelingen in dit advies over te nemen.
92. Op basis van de beschikbare informatie merkt het EDPB op dat er met betrekking tot de toegang door rechtshandavingsinstanties tot gegevens van bedrijven in de VS een vrij solide onafhankelijk toezichtmechanisme bestaat.

3.1.4 De betrokken personen moeten beschikken over doeltreffende beroepsmogelijkheden

93. Volgens de rechtspraak van het Hof moeten natuurlijke personen over een doeltreffende beroepsmogelijkheid beschikken om hun rechten te doen gelden wanneer zij menen dat deze niet worden of zijn geëerbiedigd. In het arrest Schrems I stelde het Hof: “Evenzeer eerbiedigt een regeling die niet in enige beroepsmogelijkheid voor de justitiabele voorziet om toegang tot de hem betreffende persoonsgegevens te verkrijgen, of rectificatie of verwijdering van die gegevens, de wezenlijke inhoud van het grondrecht op een effectieve voorziening in rechte zoals neergelegd in artikel 47 van het Handvest niet. Artikel 47, eerste alinea, van het Handvest schrijft immers voor dat eenieder wiens door het recht van de Unie gewaarborgde rechten en vrijheden zijn geschonden, recht heeft op een doeltreffende voorziening in rechte, met inachtneming van de in dit artikel gestelde voorwaarden.”⁹⁷

⁹¹ Ontwerpbesluit, overweging 92.

⁹² Ontwerpbesluit, bijlage VI, blz. 3.

⁹³ Ontwerpbesluit, overweging 90 en bijlage VI, p 3.

⁹⁴ Ontwerpbesluit, bijlage VI, blz. 4 en overweging 91.

⁹⁵ Ontwerpbesluit, bijlage VI, blz. 4 en overweging 91.

⁹⁶ Ontwerpbesluit, overwegingen 103 tot en met 106.

⁹⁷ Arrest Schrems I, punt 95.

94. Het ontwerpbesluit⁹⁸ en bijlage VI daarbij bevatten nadere informatie met betrekking tot mogelijke rechtsmiddelen op grond van de wetgeving, die beschikbaar zouden zijn voor natuurlijke personen wanneer overheidsinstanties onrechtmatig toegang krijgen tot hun gegevens.
95. Volgens de Commissie⁹⁹ bepaalt 5 U.S.C. § 702 (Administrative Procedure Act (APA)) in dit verband dat personen die onrechtmatig zijn behandeld door een instantie of die door een handeling van de overheid zijn benadeeld, zich tot het gerecht kunnen wenden.
96. Voorts bepaalt de Stored Communications Act (SCA) (vastgesteld als titel III van de Electronic Communications Privacy Act) dat eenieder die is benadeeld door een schending van dat hoofdstuk, waarbij het gedrag dat de schending uitmaakt bewust of opzettelijk is begaan, in een civiele procedure van de persoon of entiteit, niet zijnde de Verenigde Staten, die de schending heeft begaan, een passend redres kan vorderen¹⁰⁰. Daarnaast kan eenieder die is benadeeld door een opzettelijke schending van dat hoofdstuk of van hoofdstuk 119 bij de district courts van de Verenigde Staten een vordering tot schadevergoeding instellen tegen de Verenigde Staten¹⁰¹.
97. Bovendien bevat het ontwerpbesluit ook informatie over het recht om toegang te krijgen tot documenten van federale instanties uit hoofde van de Freedom of Information Act (FOIA)¹⁰² en verschillende andere wetten die natuurlijke personen het recht geven een rechtszaak aan te spannen tegen een overheidsinstantie of ambtenaar van de VS met betrekking tot de verwerking van hun persoonsgegevens, zoals de Wiretap Act, de Computer Fraud and Abuse Act, de Federal Torts Claim Act, de Right to Financial Privacy Act en de Fair Credit Reporting Act¹⁰³.
98. Het EDPB verwelkomt daarom de verduidelijkingen van de Commissie met betrekking tot het aantal verhaalmechanismen waarop personen een beroep kunnen doen. Het EDPB verzoekt de Commissie tevens nader toe te lichten of deze rechtsmiddelen de betrokkene in staat stellen “toegang tot de hem betreffende persoonsgegevens te verkrijgen, of rectificatie of verwijdering van die gegevens”, zoals het Hof eist.

3.1.5 Verder gebruik van de verzamelde informatie

3.1.5.1 *Verder gebruik van doorgegeven gegevens waartoe rechtshandhavingsinstanties in de VS toegang hebben*

99. Het EDPB is ingenomen met het feit dat in het ontwerpbesluit een beoordeling is opgenomen van het verdere gebruik van gegevens waartoe rechtshandhavingsinstanties in de VS toegang hebben. Het EDPB betreurt echter dat slechts één voorbeeld wordt gegeven van de gronden waarop de informatie verder kan worden verspreid¹⁰⁴. In dat verband beveelt het EDPB de Commissie aan in het ontwerpbesluit een nadere verduidelijking op te nemen van de beginselen en waarborgen die van

⁹⁸ Ontwerpbesluit, overwegingen 107 tot en met 112.

⁹⁹ Ontwerpbesluit, overweging 109.

¹⁰⁰ 18 U.S.C. § 2707.

¹⁰¹ 18 U.S.C. § 2712.

¹⁰² Ontwerpbesluit, overweging 111.

¹⁰³ Ontwerpbesluit, overweging 112.

¹⁰⁴ Ontwerpbesluit, overweging 102.

toepassing zijn op het verdere gebruik van gegevens, zoals die welke zijn opgenomen in de Privacy Act (5 U.S.C. 552a)¹⁰⁵.

3.1.5.2 Verdere doorgifte buiten de VS

100. Het EDPB merkt voorts op dat de Europese Commissie ook heeft verwezen naar verdere doorgifte door de rechtshandhavingsinstanties in de VS aan autoriteiten in derde landen, maar opnieuw alleen met betrekking tot de richtsnoeren van de minister van Justitie in verband met binnenlandse FBI-operaties (AGG-DOM)¹⁰⁶. Het EDPB is van mening dat dergelijke informatie en beoordeling van essentieel belang zijn om een alomvattende beoordeling mogelijk te maken van het beschermingsniveau dat door het Amerikaanse rechtskader en de Amerikaanse praktijken wordt geboden met betrekking tot internationale openbaarmaking en verder gebruik. Aangezien de Commissie slechts één, beperkt, voorbeeld heeft gegeven betreffende de kwestie van verdere doorgifte buiten de VS als geheel, verzoekt het EDPB de Commissie om nadere toelichting van de toepasselijke regels en waarborgen voor verdere doorgifte, verder gebruik en openbaarmaking van persoonsgegevens die voor rechtshandhavingsdoeleinden in de VS zijn verzameld en vervolgens aan derde landen, ook via internationale overeenkomsten, worden doorgegeven.

3.2 Toegang en gebruik ten behoeve van de nationale veiligheid

101. Het EDPB erkent in het algemeen dat de lidstaten een ruime beoordelingsmarge hebben in zaken van nationale veiligheid, hetgeen ook door het EHRM wordt erkend. Het EDPB wijst er ook op dat, zoals hij in zijn bijgewerkte aanbevelingen over de Europese essentiële garanties voor surveillancemaatregelen¹⁰⁷ heeft benadrukt, in artikel 6, lid 3, van het Verdrag betreffende de Europese Unie is bepaald dat de grondrechten die zijn vastgesteld in het EVRM als algemene beginselen deel uitmaken van de EU-wetgeving. Het Hof herinnert er in zijn jurisprudentie echter aan dat dit laatste, zolang de EU er niet toe is toegetreden, geen rechtsinstrument is dat formeel in de EU-wetgeving is opgenomen¹⁰⁸. Bijgevolg moet het door artikel 45 AVG vereiste beschermingsniveau voor de grondrechten worden bepaald op basis van de bepalingen van die verordening, gelezen in het licht van de grondrechten die in het EU-Handvest zijn verankerd. Evenwel hebben volgens artikel 52, lid 3, EU-Handvest de daarin vervatte rechten die overeenkomen met door het EVRM gewaarborgde rechten, dezelfde inhoud en reikwijdte als die welke door het EVRM worden toegekend. Zoals het Hof heeft opgemerkt, moet bijgevolg rekening worden gehouden met de EHRM-jurisprudentie betreffende rechten die ook in het EU-Handvest zijn opgenomen, die het minimale beschermingsniveau bepalen voor de uitlegging van de overeenkomstige rechten in het EU-Handvest¹⁰⁹. De laatste zin van artikel 52, lid 3, EU-Handvest luidt echter: “[d]eze bepaling verhindert niet dat het recht van de Unie een ruimere bescherming biedt.”
102. Daarom heeft het EDPB bij de volgende beoordeling rekening gehouden met de jurisprudentie van het EHRM, voor zover het EU-Handvest, zoals uitgelegd door het Hof, niet voorziet in een hoger beschermingsniveau dat andere eisen stelt dan de EHRM-jurisprudentie.

¹⁰⁵ Zie de richtsnoeren van de minister van Justitie in verband met binnenlandse FBI-operaties (AGG-DOM), blz. 36, deel B (1)(g).

¹⁰⁶ Ontwerpbesluit, overweging 102.

¹⁰⁷ Zie Aanbevelingen 02/2020 van het EDPB over de Europese essentiële garanties voor surveillancemaatregelen.

¹⁰⁸ Arrest Schrems II, punt 98.

¹⁰⁹ Arrest La Quadrature du Net, punt 124.

103. Verschillende rechtsinstrumenten voorzien in de mogelijkheid voor Amerikaanse inlichtingendiensten om in het rechtskader van de Verenigde Staten gegevens te verzamelen en verder te raadplegen en te verwerken.
104. Zoals de Europese Commissie in haar ontwerpbesluit in herinnering brengt, kunnen de inlichtingendiensten van de VS alleen toegang vragen tot persoonsgegevens die ten behoeve van de nationale veiligheid aan in de Verenigde Staten gevestigde organisaties zijn doorgegeven als dit bij wet is toegestaan, met name op grond van de Foreign Intelligence Surveillance Act (FISA) of wettelijke bepalingen die toegang toestaan door middel van *national security letters* (NSL)¹¹⁰. Krachtens Executive Order 12333 hebben Inlichtingendiensten van de VS ook mogelijkheden om persoonsgegevens buiten de Verenigde Staten te verzamelen, waaronder mogelijk persoonsgegevens in doorvoer tussen de Unie en de Verenigde Staten¹¹¹.
105. Met betrekking tot de specifieke regelingen voor gegevensverzameling, in het bijzonder sectie 702 FISA en EO 12333, voorziet EO 14086 nu in nieuwe regels om de waarborgen voor de activiteiten van de VS op het gebied van SIGINT te versterken. Deze algemene regels zijn horizontaal van toepassing en moeten verder worden uitgevoerd via beleidsmaatregelen en procedures van de instanties die ze omzetten in concrete aanwijzingen voor dagelijkse operaties¹¹². EO 14086 is grotendeels in de plaats gekomen van de vorige presidentiële beleidsrichtlijn 28 (“PPD-28”)¹¹³.
106. Voor een beoordeling van het rechtskader voor de verzameling van, de toegang tot en de verdere verwerking van gegevens ten behoeve van de nationale veiligheid is het dus van belang het specifieke rechtskader voor de verzameling van gegevens binnen en buiten de VS te onderzoeken, d.w.z. sectie 702 FISA en EO 12333, die als zodanig niet zijn gewijzigd sinds de vorige evaluatie van het privacyschild, rekening houdend met het feit dat het nieuwe Executive Order 14086 voorziet in waarborgen die ook moeten worden toegepast in het kader van de verzameling van gegevens op grond van specifieke teksten zoals sectie 702 FISA en EO 12333.

3.2.1 Garantie A — De verwerking moet in overeenstemming zijn met de wet en gebaseerd zijn op duidelijke, nauwkeurige en toegankelijke regels

107. Voor zijn beoordeling van de algemene opzet van het verzamelen van gegevens ten behoeve van de nationale veiligheid wenst het EDPB te herinneren aan de eerste van de vier zogenaamde “Europese essentiële garanties”, volgens welke “de verwerking moet gebaseerd zijn op duidelijke, precieze en toegankelijke regels”¹¹⁴.
108. Volgens vaste rechtspraak van het Hof moet elke beperking van het recht op bescherming van persoonsgegevens bij wet zijn bepaald en moet de rechtsgrond die de inmenging in dat recht toestaat, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht bepalen¹¹⁵. Het Hof

¹¹⁰ Ontwerpbesluit, overweging 115.

¹¹¹ Ontwerpbesluit, overweging 117.

¹¹² Ontwerpbesluit, overweging 120.

¹¹³ Bij EO 14086 wordt PPD-28 ingetrokken, met uitzondering van de secties 3 en 6 van die richtlijn en de gerubriceerde bijlage bij die richtlijn, die van kracht blijven. Zie het presidentieel memorandum inzake nationale veiligheid van 7 oktober 2022.

¹¹⁴ Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, vastgesteld op 10 november 2020. Zie arrest Schrems II, de punten 175 en 180, Advies 1/15 (PNR-overeenkomst EU-Canada) van 26 juli 2017, punt 139 en de aldaar aangehaalde rechtspraak.

¹¹⁵ Arrest Schrems II van het Hof, punten 174-175 en de aldaar aangehaalde rechtspraak. Zie ook, wat de toegang door overheidsinstanties van de lidstaten betreft, zaak C-623/17, Privacy International, ECLI:EU:C:2020:790

herinnerde er ook aan dat wetgeving wettelijk verbindend moet zijn naar intern recht¹¹⁶. In dit verband verduidelijkt de rechtspraak van het EHRM dat de term “wet” in zijn materiële en niet in zijn formele betekenis moet worden opgevat. Het kan gaan om lagere wetten en regelgevende maatregelen die door regelgevende beroepsorganisaties worden genomen op grond van onafhankelijke regelgevende bevoegdheden die door het parlement aan hen zijn gedelegeerd, en zelfs om ongeschreven recht. Om een “wet” te zijn, moet een rechtsnorm ten minste voldoende toegankelijk zijn en voldoende nauwkeurig zijn geformuleerd¹¹⁷.

109. De vereiste mate van nauwkeurigheid moet worden afgemeten aan de omvang van de beperking van het recht¹¹⁸. Wat de “voorzienbaarheid” van het recht betreft, herinnerde het EHRM er in de zaak Zakharov bovendien aan dat in het kader van geheime surveillancemaatregelen, zoals het aftappen van communicatie, voorzienbaarheid niet kan betekenen dat een persoon moet kunnen voorzien wanneer de autoriteiten zijn communicatie waarschijnlijk zullen aftappen, zodat hij zijn gedrag dienovereenkomstig kan aanpassen. Duidelijke en gedetailleerde regels inzake geheime surveillancemaatregelen zijn echter essentieel om het risico van willekeur te voorkomen wanneer een bevoegdheid van de uitvoerende macht in het geheim wordt uitgeoefend. “Het nationale recht moet voldoende duidelijk zijn om de natuurlijke personen voldoende duidelijkheid te verschaffen over de omstandigheden waarin en de voorwaarden waaronder de overheid bevoegd is van dergelijke maatregelen gebruik te maken”¹¹⁹.
110. Bovendien heeft het Hof verduidelijkt dat de beoordeling van het toepasselijke recht van een derde land zich moet toespitsen op de vraag of natuurlijke personen zich voor de rechter op dit recht kunnen beroepen. De aan betrokkenen verleende rechten moeten met name voor beroep vatbaar zijn en personen moeten rechten krijgen die zij voor de rechtbanken tegenover de overheidsdiensten kunnen afdwingen¹²⁰, hetgeen niet het geval was in het kader van het vorige PPD-28. Presidentieel besluit EO 14086 dat, zoals het EDPB begrijpt, geacht wordt binnen de rechtsorde van de VS dezelfde rechtsgevolgen te hebben als PPD-28 (d.w.z. bindend voor de uitvoerende macht), voorziet nu in rechten die tegenover overheidsdiensten kunnen worden afgedwongen. Een uitvoerige beoordeling van de nieuwe afdwingbare rechten van de betrokkenen wordt gegeven in het hoofdstuk over verhaalsmogelijkheden.
111. De overwegingen 114 tot en met 152 van het ontwerpbesluit en bijlage VII bevatten een samenvatting van enkele aspecten van het geldende rechtskader, de beperkingen inzake verzameling, bewaring en verspreiding, naleving en toezicht, transparantie en verhaalsmiddelen. Het Amerikaanse rechtssysteem voor inlichtingenactiviteiten bestaat uit een aantal verschillende documenten, waaronder verslagen, beleidsmaatregelen en procedures van afzonderlijke instanties. In dat opzicht is de evaluatie van het EDPB gericht op een beperkt aantal punten die het van cruciaal belang acht.
112. Volgens de overwegingen 115 tot en met 119 van het ontwerpbesluit kan toegang tot doorgegeven persoonsgegevens door de Amerikaanse nationale veiligheidsautoriteiten alleen plaatsvinden op grond van de FISA, op grond van andere wettelijke bepalingen (12 U.S.C. § 3414, 15 U.S.C. § 1681u-

(hierna het “arrest Privacy International van het Hof” genoemd), punt 65; en arrest La Quadrature du Net van het Hof, punt 175.

¹¹⁶ Arrest Privacy International van het Hof, punt 68.

¹¹⁷ EHRM, Sunday Times/UK (No. 1), 26 april 1979, CE:ECHR:1979:0426JUD000653874 (hierna “EHRM-arrest Sunday Times/UK No. 1” genoemd), punt 49.

¹¹⁸ EHRM-arrest Sunday Times/UK No. 1, punt 49.

¹¹⁹ EHRM, Zakharov/Rusland, 4 december 2015 (hierna “EHRM-arrest Zakharov” genoemd), punt 229.

¹²⁰ Arrest Schrems II van het Hof, punt 181.

1681v en 18 U.S.C. § 2709) of, in verband met persoonsgegevens in doorvoer, op grond van EO 12333. Uit de overwegingen 116 en 118 van het ontwerpbesluit blijkt dat de Commissie haar beoordeling, in verband met de toegang tot persoonsgegevens door de Amerikaanse nationale veiligheidsautoriteiten, toespitst op de secties 105, 302, 402, 501 en 702 FISA (buitenlandse inlichtingenactiviteiten gericht op niet-Amerikanen die zich buiten de VS bevinden) en EO 12333 (buitenlandse inlichtingenactiviteiten betreffende persoonsgegevens in doorvoer), als zijnde het relevantst. Het advies van het EDPB beperkt zich derhalve tot de beoordeling van deze bepalingen door de Commissie, rekening houdend met de in EO 14086 vastgestelde beperkingen en waarborgen¹²¹.

113. In dit verband moet worden opgemerkt dat alle in het ontwerpbesluit genoemde rechtsinstrumenten toegankelijk zijn voor het grote publiek (in de VS en daarbuiten) en online beschikbaar zijn. Voorts zijn de in het EO neergelegde voorschriften bindend voor alle inlichtingendiensten¹²² en gelden zij op horizontale wijze voor alle activiteiten op het gebied van buitenlandse inlichtingen.
114. Het begrip “signals intelligence” (SIGINT — inlichtingen uit het berichtenverkeer) wordt niet gedefinieerd in EO 14086. In EO 14086 wordt verwezen naar de definities in EO 12333 voor het vaststellen van de reikwijdte van buitenlandse inlichtingen of contraspionage, die ruim gedefinieerd zijn. Hoewel in dit verband is aangevoerd dat EO 12333 sinds de invoering van de FISA alleen kan worden gebruikt voor het verzamelen van gegevens buiten het grondgebied van de VS, herinnert het EDPB eraan dat EO 12333 zelf, dat onaangetast blijft, onvoldoende details bevat over het geografische toepassingsgebied, de mate waarin gegevens kunnen worden verzameld, bewaard of verder verspreid, of over de aard van de strafbare feiten die aanleiding kunnen geven tot surveillance of het soort informatie dat kan worden verzameld of gebruikt. In beginsel kan het verzamelen van buitenlandse inlichtingen binnen de reikwijdte van EO 12333 naar goeddunken van de Amerikaanse president plaatsvinden¹²³. Volgens het EDPB heeft EO 14086 echter voornamelijk tot doel de grenzen voor te schrijven voor de verzameling en verwerking van persoonsgegevens in het kader van buitenlandse inlichtingen, ongeacht welk surveillanceprogramma wordt gebruikt en waar de gegevens vandaan komen. Het EDPB gaat er derhalve van uit dat de aanvullende waarborgen waarin EO 14086 voorziet, ook gelden in het kader van surveillanceprogramma’s die van toepassing zijn op persoonsgegevens in doorvoer in het kader van EO 12333¹²⁴.
115. In dit verband worden in EO 14086 twaalf legitieme doelstellingen genoemd die moeten worden nagestreefd bij het verzamelen van SIGINT en vijf doelstellingen waarvoor geen SIGINT mogen worden verzameld¹²⁵, alsmede zes legitieme doelstellingen voor het gebruik van bulksgewijs verzamelde gegevens¹²⁶. Sommige daarvan zijn vrij gedetailleerd (bv. “redding van gijzelaars”), andere zijn algemener (bv. “mondiale veiligheid”). Presidentieel besluit EO 14086 bevat ook een lijst van verboden doelstellingen, waaronder met name de onderdrukking of beperking van “rechtmatige privacybelangen”¹²⁷. In EO 14086 is ook bepaald dat de president van de Verenigde Staten de

121 Bij presidentieel besluit EO 14086 wordt PPD-28 ingetrokken, met uitzondering van de secties 3 en 6 van die richtlijn en de gerubriceerde bijlage bij die richtlijn, die van kracht blijven. Zie [het presidentieel memorandum inzake nationale veiligheid van 7 oktober 2022](#).

122 Ontwerpbesluit, overweging 120.

123 Krachtens artikel II van de grondwet van de Verenigde Staten valt de verantwoordelijkheid voor het waarborgen van de nationale veiligheid, waaronder met name het vergaren van buitenlandse inlichtingen, onder de bevoegdheid van de president als opperbevelhebber van de strijdkrachten.

124 Ontwerpbesluit, overweging 134.

125 EO 14086, sectie 2, (b), (ii), A, 1 tot en met 5.

126 Ontwerpbesluit, overweging 134 en EO 14086, sectie 2, (c), (ii).

127 EO 14086, sectie 2, (b), (ii), (A), (2).

mogelijkheid heeft om andere doelstellingen toe te voegen aan de lijst waarvoor verzameling is toegestaan, die bij besluit van de president niet aan het publiek mogen worden vrijgegeven indien de president van oordeel is dat dit een risico voor de nationale veiligheid van de Verenigde Staten zou inhouden¹²⁸. Dergelijke actualiseringen kunnen alleen worden toegestaan “in het licht van nieuwe vereisten van nationale veiligheid”.

116. De inlichtingendiensten kunnen de doelstellingen op zich niet gebruiken om het verzamelen van SIGINT te rechtvaardigen, maar moeten voor operationele doeleinden verder worden uitgewerkt tot meer concrete prioriteiten waarvoor SIGINT kunnen worden verzameld. In EO 14086 wordt de procedure voor de validering van de prioriteiten waarvoor SIGINT kunnen worden verzameld, nader omschreven¹²⁹. Het EDPB begrijpt dat het proces om de gevalideerde inlichtingenprioriteiten vast te stellen in beginsel afhangt van de directeur van de inlichtingendiensten en erkent dat het in de regel de beoordeling van de Civil Liberties Protection Officer (CLPO, functionaris voor de bescherming van de burgerlijke vrijheden) van het Office of the Director of National Intelligence (ODNI, bureau van de directeur van de nationale inlichtingendienst) moet omvatten, waarmee de directeur het oneens kan zijn, in welk geval die laatste de beoordeling van de CLPO en het standpunt van de directeur opneemt wanneer hij of zij het National Intelligence Priorities Framework (NIPF) (nationaal kader voor de prioriteiten op het gebied van inlichtingen) aan de president voorlegt¹³⁰.
117. Het EDPB merkt echter ook op dat volgens de definitie van “gevalideerde inlichtingenprioriteit”, dergelijke prioriteiten voor de meeste activiteiten van de Verenigde Staten in verband met het verzamelen van SIGINT¹³¹ een prioriteit inhouden die is gevalideerd overeenkomstig sectie 2, (b), (iii) EO (beschreven in het vorige punt). In “beperkte omstandigheden” kan het validatieproces verschillen van dit proces. In dat geval kan de president of het hoofd van een onderdeel van de inlichtingendiensten “voor zover haalbaar” een prioriteit vaststellen in overeenstemming met de criteria van dezelfde sectie 2, (b), (iii), (A), (1)-(3), waaronder de eis dat op passende wijze rekening moet worden gehouden met de privacy en de burgerlijke vrijheden van alle personen, maar zonder tussenkomst van de CLPO.
118. In EO 14086 wordt bovendien onderstreept dat activiteiten in verband met het verzamelen van SIGINT zo goed mogelijk moeten worden toegesneden om een gevalideerde inlichtingenprioriteit te bevorderen, en dat de inlichtingendiensten de beschikbaarheid, haalbaarheid en geschiktheid van andere, minder indringende bronnen in overweging moeten nemen. Het EO bevat ook algemene vereisten inzake noodzakelijkheid en evenredigheid¹³².
119. Voorts creëert EO 14086 uit hoofde van sectie 5, (h), een recht om in aanmerking komende klachten in te dienen bij de CLPO en om de besluiten van de CLPO te laten toetsen door de Data Protection Review Court overeenkomstig het in sectie 3 van dat EO vastgestelde verhaalmechanisme.
120. De tekst van de FISA lijkt duidelijker en preciezer dan EO 12333 wat betreft het soort inlichtingenoperaties dat kan worden opgedragen. De FISA en EO 12333 moeten nu worden toegepast in het licht van EO 14086, met inachtneming van de beginselen van noodzakelijkheid en evenredigheid.

¹²⁸ EO 14086, sectie 2, (b), (i), (B).

¹²⁹ Ontwerpbesluit, overweging 129.

¹³⁰ EO 14086, sectie 2, (b), (iii), (B).

¹³¹ EO 14086, sectie 4, (n).

¹³² EO 14086, sectie 2, (c), (i), (A) en (B).

121. De in EO 14086 neergelegde vereisten moeten verder worden uitgevoerd via beleidsmaatregelen en procedures van instanties die ze omzetten in concrete richtsnoeren voor dagelijkse operaties. In dit verband geeft EO 14086 de Amerikaanse inlichtingendiensten maximaal een jaar de tijd om hun bestaande beleidsmaatregelen en procedures bij te werken (d.w.z. uiterlijk 7 oktober 2023) en in overeenstemming te brengen met de eisen van het EO. Die bijgewerkte beleidsmaatregelen en procedures moeten worden ontwikkeld in overleg met de minister van Justitie, de CLPO en de Privacy and Civil Liberties Oversight Board (PCLOB) en zoveel mogelijk openbaar worden gemaakt¹³³.
122. Het EDPB zou graag zien dat niet alleen de inwerkingtreding maar ook de vaststelling van het besluit afhankelijk wordt gesteld van onder meer de vaststelling van geactualiseerde beleidsmaatregelen en procedures door alle Amerikaanse inlichtingendiensten ter uitvoering van EO 14086. Het EDPB beveelt de Commissie aan deze geactualiseerde beleidsmaatregelen en procedures te beoordelen en deze beoordeling met het EDPB te delen.
123. Tot slot merkt het EDPB met betrekking tot de bewaring van de doorgegeven gegevens die ten behoeve van de nationale veiligheid zijn verzameld, op dat EO 14086 waarborgt dat de regels die gelden voor persoonsgegevens van Amerikanen ook van toepassing zijn op de persoonsgegevens van niet-Amerikanen¹³⁴. Uit het ontwerpbesluit blijkt dat deze regels zijn opgenomen in sectie 309 van de Intelligence Authorization Act for Fiscal Year 2015¹³⁵, waarin een maximale bewaartermijn van vijf jaar is vastgesteld voor in beginsel alle niet-openbare telefonische of elektronische communicatie die zonder toestemming van de persoon is verkregen. Het EDPB beveelt in dit verband aan dat de Commissie meer duidelijkheid verschaft over haar beoordeling van de bewaringsregels die van toepassing zijn op persoonsgegevens van Amerikanen in het besluit.

3.2.2 Garantie B — De noodzakelijkheid en evenredigheid van de nagestreefde legitieme doelstellingen moeten worden aangetoond

3.2.2.1 Horizontale garanties in het nieuwe Executive Order 14086 – Noodzakelijkheid en evenredigheid

124. Het nieuwe EO 14086, dat PPD-28 in grote lijnen vervangt, heeft tot doel regels vast te stellen om de garanties voor de Amerikaanse activiteiten op het gebied van SIGINT te versterken, en die regels verder te laten uitvoeren door de onderdelen van de inlichtingendiensten in hun interne beleidsmaatregelen en procedures.
125. EO 14086 introduceert twee nieuwe voorschriften in de Amerikaanse wetgeving die aansluiten bij de voorschriften waaraan het Hof in zijn arrest Schrems II heeft herinnerd, namelijk dat activiteiten op het gebied van SIGINT alleen mogen worden uitgevoerd voor zover dat nodig is om een gevalideerde prioritaire inlichtingenverzameling te bevorderen en alleen voor zover en op een wijze die evenredig is aan de gevalideerde inlichtingenprioriteit¹³⁶.
126. Het EDPB gaat ervan uit dat deze elementen zijn opgenomen om de beginselen van noodzakelijkheid en evenredigheid te weerspiegelen waarin het EU-recht en de jurisprudentie van het Hof en van het EHRM voorzien en die ervoor moeten zorgen dat het verzamelen en verwerken van gegevens beperkt blijft tot hetgeen noodzakelijk en evenredig is.

¹³³ EO 14086, sectie 2, (c), (iv), (B) en (C).

¹³⁴ Ontwerpbesluit, overweging 150.

¹³⁵ Ontwerpbesluit, voetnoot 272.

¹³⁶ EO 14086, sectie 2, (a), (ii), A en B.

127. In dit verband herinnert het EDPB aan de procedure voor de validatie van prioriteiten op het gebied van inlichtingen en de mogelijke afwijking ervan (zie de punten 116 en 117).
128. Voorts merkt het EDPB op dat deze beginselen van noodzakelijkheid en evenredigheid die in het EO zijn opgenomen binnen een jaar in de beleidsmaatregelen en procedures van elk onderdeel van de inlichtingendiensten operationeel moeten worden gemaakt en toegepast¹³⁷.

3.2.2.2 Specifieke waarborgen voor het verzamelen van SIGINT

129. Het EDPB merkt ook op dat EO 14086 voorziet in beperkingen met betrekking tot de doelstellingen waarvoor persoonsgegevens wel en niet kunnen worden verzameld, in het kader van het verzamelen van SIGINT¹³⁸.
130. Het EDPB is ingenomen met het feit dat het EO bepaalt dat gericht verzamelen voorrang moet krijgen boven bulksgewijs verzamelen¹³⁹. In het kader van het verzamelen van SIGINT voorziet het EO in een lijst van twaalf doelstellingen waarvoor gegevens kunnen worden verzameld, die verder moeten worden uitgewerkt tot inlichtingenprioriteiten (zie punt 117), alsook in een lijst van vijf doelstellingen waarvoor geen activiteiten inzake het verzamelen van SIGINT mogen worden verricht¹⁴⁰. In beginsel vormen deze bepalingen een garantie voor de noodzakelijkheid van het verzamelen van gegevens.
131. Het EDPB herinnert er echter aan dat EO 14086 ook bepaalt dat de president van de Verenigde Staten andere doelstellingen aan de lijst kan toevoegen (zie de punten 114 en 115)¹⁴¹.

3.2.2.3 Specifieke garanties voor bulksgewijs verzamelen

132. In zijn arrest Schrems I onderstreepte het Hof dat “de bescherming van het grondrecht op eerbiediging van het privéleven op het niveau van de Unie [vereist] dat de uitzonderingen op de bescherming van persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven”¹⁴² en oordeelde het dat “een regeling op grond waarvan de autoriteiten veralgemeend toegang kunnen krijgen tot de inhoud van elektronische communicatie [moet] worden beschouwd als een aantasting van de wezenlijke inhoud van het grondrecht op eerbiediging van het privéleven zoals door artikel 7 van het Handvest gewaarborgd”.
133. In de zaak Schrems II¹⁴³ heeft het Hof met betrekking tot zijn analyse van bulksgewijs verzamelen in het licht van de gecombineerde lezing van EO 12333 en PPD-28, en met name in de punten 183 tot en met 185, zoals hierboven in herinnering gebracht, benadrukt dat de mogelijkheid “om in het kader van op E.O. 12333 gebaseerde surveillanceprogramma’s toegang tot gegevens te krijgen tijdens hun doorgifte naar de Verenigde Staten, zonder dat die toegang aan enig gerechtelijk toezicht is onderworpen, [...] hoe dan ook niet op voldoende duidelijke en nauwkeurige wijze de reikwijdte [afbakent] van een dergelijke bulksgewijze verzameling van persoonsgegevens”.
134. Het EDPB merkt derhalve op dat het Hof bulksgewijze verzameling niet principieel heeft uitgesloten, maar in zijn arrest Schrems II heeft overwogen dat een dergelijke bulksgewijze verzameling slechts

¹³⁷ EO 14086, sectie 2, (c), (iv), B.

¹³⁸ EO 14086, sectie 2, (b), (i), A, 1 tot en met 12.

¹³⁹ EO 14086, sectie 2, (c), (ii), A.

¹⁴⁰ EO 14086, sectie 2, (b), (ii), A, 1 tot en met 5.

¹⁴¹ EO 14086, sectie 2, (b), (i), B.

¹⁴² Arrest Schrems I van het Hof, punt 92.

¹⁴³ Arrest Schrems II van het Hof.

rechtmatig kan plaatsvinden indien er voldoende duidelijke en nauwkeurige grenzen zijn om de reikwijdte ervan af te bakenen.

135. Het EDPB erkent tevens dat EO 14086 weliswaar PPD-28 vervangt, maar voorziet in nieuwe waarborgen en beperkingen voor het verzamelen en gebruiken van buiten de VS verzamelde gegevens, aangezien de beperkingen van de FISA of andere meer specifieke Amerikaanse wetten niet van toepassing zijn.
136. Met betrekking tot de bulksgewijze verzameling van gegevens neemt het EDPB er kennis van dat EO 14086 bepaalt dat de bulksgewijze verzameling van gegevens toegestaan blijft. Het EDPB onderstreept dat de definitie van bulksgewijze verzameling namelijk dezelfde blijft als in het vorige PPD-28: onder “bulksgewijze” verzamelde SIGINT wordt verstaan de toegestane verzameling van grote hoeveelheden SIGINT die om technische of operationele redenen worden verkregen zonder gebruik van discriminanten (bijvoorbeeld zonder gebruik van specifieke identificatoren of selectietermen)¹⁴⁴.
137. Sinds het arrest Schrems II heeft het Hof niet meer precies aangegeven welke waarborgen vereist zijn om bulksgewijze verzameling mogelijk te maken. Het EDPB herinnert er echter aan dat het EHRM belangrijke arresten heeft gewezen over de bulksgewijze verzameling van gegevens en de desbetreffende waarborgen in dit verband.
138. Het EDPB herinnert eraan dat bulksgewijze verzameling, waarbij zonder onderscheid grote hoeveelheden gegevens kunnen worden verzameld, grotere risico's voor de betrokkenen inhoudt¹⁴⁵ dan gerichte verzameling en dat dus aanvullende waarborgen moeten worden geboden.
139. Het EDPB merkt tevens op dat het Hof verdere jurisprudentie heeft ontwikkeld betreffende het bewaren van verkeers- en locatiegegevens en de latere toegang tot deze door telecommunicatie-exploitanten bewaarde gegevens, onder meer ten behoeve van de nationale veiligheid, die, hoewel die jurisprudentie in deze context niet rechtstreeks toepasselijk kan worden geacht, tot op zekere hoogte relevant zou kunnen zijn voor de onderhavige beoordeling van bulksgewijze verzameling in het kader van EO 12333.

1) Doelbinding

140. Het EO bepaalt dat bulksgewijze verzameling alleen mag plaatsvinden na een vaststelling dat de informatie die nodig is om een gevalideerde inlichtingenprioriteit te bevorderen niet redelijkerwijs kan worden verkregen door gerichte verzameling¹⁴⁶, en dat het onderdeel van de inlichtingendiensten redelijke methoden en technische maatregelen moet toepassen om de verzamelde gegevens te beperken tot wat nodig is om een gevalideerde inlichtingenprioriteit te bevorderen, waarbij het verzamelen van niet-pertinente informatie tot een minimum wordt beperkt¹⁴⁷. Naast deze waarborgen erkent het EDPB ook dat bulksgewijs verzamelde gegevens moeten worden gebruikt om een of meer van de zes genoemde doelstellingen te verwezenlijken¹⁴⁸. Het EDPB benadrukt voorts dat deze doelstellingen weliswaar gedetailleerder zijn dan die van het vorige PPD-28, dat in het algemeen door

¹⁴⁴ EO 14086, sectie 4, (b).

¹⁴⁵ Zie bijvoorbeeld EHRM (Grote Kamer), Big Brother Watch e.a./Verenigd Koninkrijk, 25 mei 2021 (hierna het “EHRM-arrest Big Brother Watch” genoemd), overweging 363, waarin het Hof aangeeft dat het er niet van overtuigd is dat de verkrijging van verwante communicatiegegevens door middel van bulksgewijze onderschepping noodzakelijkerwijs minder indringend is dan de verkrijging van inhoud.

¹⁴⁶ EO 14086, sectie 2, (c), (ii), (A).

¹⁴⁷ EO 14086, sectie 2, (c), (ii), (A).

¹⁴⁸ EO 14086, sectie 2, (c), (ii), (B).

EO 14086 is vervangen, maar dat de omvang van dergelijke verzamelmogelijkheden potentieel breed blijft, d.w.z. dat zij grote hoeveelheden gegevens omvatten.

141. Het EDPB herinnert er hier tevens aan dat EO 14086 ook bepaalt dat de president van de Verenigde Staten andere doelstellingen aan de lijst kan toevoegen (zie punt 115)¹⁴⁹.

2) Voorafgaande onafhankelijke toestemming

142. Het EDPB benadrukt dat het EHRM veel belang hecht aan voorafgaande onafhankelijke toestemming in het kader van het bulksgewijs verzamelen van gegevens ten behoeve van de nationale veiligheid. Het EHRM oordeelde met name dat, om het risico van misbruik van de bevoegdheid tot het bulksgewijs onderscheppen van gegevens tot een minimum te beperken, het EHRM van oordeel is dat de procedure moet worden onderworpen aan “eind-tot-eind-waarborgen”, hetgeen betekent dat op nationaal niveau in elke fase van de procedure de noodzakelijkheid en evenredigheid van de genomen maatregelen moeten worden beoordeeld; dat voor bulksgewijze onderschepping aan het begin, wanneer het voorwerp en de reikwijdte van de operatie worden bepaald, een onafhankelijke toestemming moet worden verleend; en dat de operatie moet worden onderworpen aan toezicht en onafhankelijke toetsing achteraf. Volgens het EHRM zijn dit fundamentele waarborgen die de hoeksteen zullen vormen van elke regeling voor bulksgewijze onderschepping die in overeenstemming is met artikel 8¹⁵⁰.
143. Het EDPB wijst ook op de volgende alinea van dit arrest in de Grote Kamer, waarin verder wordt benadrukt dat het EHRM “het er met de kamer over eens is dat toestemming van de rechter weliswaar een “belangrijke waarborg tegen willekeur”, maar geen “noodzakelijk vereiste” is (zie de punten 318 tot en met 320 van het arrest van de kamer). Niettemin moet voor de bulksgewijze onderschepping toestemming worden verleend door een onafhankelijke instantie; dat wil zeggen een instantie die onafhankelijk is van de uitvoerende macht”¹⁵¹.
144. In dit verband merkt het EDPB op dat het EO niet voorziet in een dergelijke onafhankelijke voorafgaande toestemming voor de bulksgewijze verzameling, en dat ook EO 12333 daar niet in voorziet (zie het onderstaande punt over EO 12333).

3) Bewaringsregels

145. Het EDPB herinnert eraan dat een andere belangrijke reeks waarborgen de regels voor de duur van het verzamelen en bewaren van gegevens zijn. In dit verband benadrukte het EHRM dat het nationale recht een grens moet stellen aan de duur van de onderschepping, de procedure die moet worden gevolgd voor het onderzoek, het gebruik en de bewaring van de verkregen gegevens, de voorzorgsmaatregelen die moeten worden genomen bij de mededeling van de gegevens aan andere partijen, en de omstandigheden waarin onderschepte gegevens kunnen of moeten worden gewist of vernietigd¹⁵² aangezien deze waarborgen evenzeer relevant zijn voor bulksgewijze onderschepping¹⁵³.
146. In dit verband heeft het EDPB begrepen dat het EO voorziet in regels betreffende de bewaring van gegevens voor persoonsgegevens die zijn verzameld via SIGINT, onder meer bulksgewijs¹⁵⁴. Het EDPB

¹⁴⁹ EO 14086, sectie 2, (c), (ii), (C).

¹⁵⁰ Zie EHRM-arrest Big Brother Watch, punt 350.

¹⁵¹ EHRM-arrest Big Brother Watch, punt 351.

¹⁵² EHRM-arrest Big Brother Watch, punt 348.

¹⁵³ EHRM-arrest Big Brother Watch, punt 348.

¹⁵⁴ EO 14086, sectie 2, (c), (iii), A, (2), (a)-(c).

merkt op dat volgens sectie 2, (c), (iii), (A), EO 14086 elk onderdeel van de inlichtingendiensten dat via SIGINT verzamelde persoonsgegevens verwerkt, beleidsmaatregelen en procedures moet vaststellen en toepassen die erop gericht zijn de verspreiding en bewaring van via SIGINT verzamelde persoonsgegevens tot een minimum te beperken. Deze regels voorzien echter niet in een specifieke bewaartermijn, maar verwijzen in het algemeen naar dezelfde toepasselijke regels voor de bewaring van gegevens over Amerikaanse personen en naar situaties waarin de bewaartermijn nog niet definitief is vastgesteld. Het EDPB is dan ook bezorgd dat deze bewaartermijnen, zoals voor gerichte verzameling (zie punt 122), in dit EO niet duidelijk worden omschreven met betrekking tot bulksgewijs verzamelde gegevens. Het EDPB verzoekt de Commissie om haar beoordeling van de noodzakelijkheid en evenredigheid van de bewaartermijnen die gelden voor Amerikanen en de beschikbare informatie over bewaartermijnen in de praktijk wanneer de bewaartermijn niet definitief is vastgesteld in het Amerikaans recht, mee te delen, aangezien het ontwerpbesluit in zijn huidige vorm deze algemene regel slechts in een enkel kort punt¹⁵⁵ en een voetnoot¹⁵⁶ vermeldt, waardoor niet kan worden bepaald of deze bewaartermijnen noodzakelijk en evenredig zijn. Aangezien dit, zoals het EHRM heeft onderstreept, voor betrokkenen een cruciale waarborg is om hun rechten te kunnen uitoefenen in een kader waarin een bijzonder indringende maatregel wordt genomen om hun gegevens te verzamelen, roept het EDPB de Europese Commissie op om meer duidelijkheid te verschaffen over de verschillende bewaartermijnen in de praktijk.

4) Waarborgen betreffende “verspreiding”

147. Tevens herinnert het EDPB eraan dat het EHRM, om de doeltreffendheid van de noodzakelijkheid en evenredigheid en het doelbindingsbeginsel te waarborgen, ook het belang heeft erkend van bij wet vastgestelde regels betreffende de verdere verspreiding van de verzamelde gegevens, ook in het kader van de bulksgewijze verzameling¹⁵⁷.
148. In sectie 2, (c), (iii), (A), (1), (c), EO 14086 is bepaald dat informatie over niet-Amerikanen die in het kader van SIGINT-activiteiten is verzameld, alleen mag worden verspreid indien een bevoegde en naar behoren opgeleide persoon er redelijkerwijs van overtuigd is dat de persoonlijke informatie op passende wijze zal worden beschermd en dat de ontvanger de informatie moet kennen.
149. Hiermee rekening houdend, begrijpt het EDPB dat de bepalingen betreffende verspreiding krachtens EO 14086 evenmin voorzien in een uitdrukkelijk verbod op verspreiding voor andere doeleinden dan de nationale veiligheid wanneer het gaat om verspreiding onder de bevoegde Amerikaanse autoriteiten¹⁵⁸. Het EDPB roept de Commissie op de toepasselijke regels en waarborgen in dit geval verder te verduidelijken.
150. Het EDPB vreest derhalve dat de door de bevoegde autoriteiten van de inlichtingendiensten verkregen gegevens vervolgens zouden kunnen worden verspreid onder bevoegde autoriteiten van de VS met het oog op de bestrijding van criminaliteit, met inbegrip van ernstige strafbare feiten, in het kader van strafrechtelijke onderzoeken, waardoor rechtshandavingsinstanties zonder verdere specifieke beperkingen over gegevens kunnen beschikken die zij niet rechtstreeks zouden mogen verzamelen, en verzoekt de Commissie dit punt nader te beoordelen.

¹⁵⁵ Ontwerpbesluit, punt 150.

¹⁵⁶ Ontwerpbesluit, voetnoot 271.

¹⁵⁷ EHRM-arrest Big Brother Watch, punt 348.

¹⁵⁸ EO 14086, sectie 2, (c), (iii), (A), (1).

151. In het specifieke kader van verdere doorgifte (verspreiding aan ontvangers buiten de regering van de Verenigde Staten, met inbegrip van een buitenlandse regering of internationale organisatie¹⁵⁹) herinnert het EDPB eraan dat hij van mening is dat de bescherming van gegevens ook in het kader van verdere doorgifte, met inbegrip van verdere doorgifte op het gebied van de nationale veiligheid, moet worden gehandhaafd¹⁶⁰.
152. In dit verband voorziet het EO in een aantal waarborgen, namelijk het vereiste om terdege rekening te houden met het doel van de verspreiding — zonder echter uitdrukkelijk te eisen dat het doel van de verspreiding ook de bescherming van de nationale veiligheid moet dienen —, de aard en de omvang van de verspreide persoonsgegevens en de mogelijke schadelijke gevolgen voor de betrokken persoon of personen, alvorens de gegevens te verspreiden.
153. Hoewel het EDPB erkent dat sommige van deze waarborgen, met name dat rekening moet worden gehouden met de “mogelijke schadelijke gevolgen”¹⁶¹ voor de betrokkene(n), in overeenstemming zijn met een aantal vereisten van het EVRM, benadrukt hij ook dat het EHRM voorts een juridisch bindende verplichting vereist om te analyseren en vast te stellen of de buitenlandse ontvanger van inlichtingen een aanvaardbaar minimumniveau van waarborgen biedt¹⁶², hetgeen het EDPB niet uitdrukkelijk terugvindt in de bepalingen van het EO betreffende de verspreiding onder buitenlandse ontvangers. Het EDPB verzoekt de Commissie derhalve dit element nader te beoordelen.
154. Het EDPB merkt tevens op dat de Europese Commissie in het kader van haar beoordeling van de adequaatheid geen rekening heeft gehouden met het bestaan van internationale overeenkomsten met derde landen of internationale organisaties die kunnen voorzien in specifieke bepalingen voor de internationale doorgifte van persoonsgegevens door inlichtingendiensten aan derde landen. Het EDPB is van mening dat de sluiting van bilaterale of multilaterale overeenkomsten met derde landen met het oog op samenwerking op het gebied van inlichtingen het beoordeelde rechtskader voor gegevensbescherming waarschijnlijk zal beïnvloeden.
155. Het EDPB verzoekt de Europese Commissie derhalve te verduidelijken of dergelijke overeenkomsten bestaan, onder welke voorwaarden zij kunnen worden gesloten en te beoordelen of de bepalingen van internationale overeenkomsten van invloed kunnen zijn op het beschermingsniveau dat door het rechtskader en de praktijken met betrekking tot verdere doorgifte ten behoeve van de nationale veiligheid wordt verstrekt aan persoonsgegevens die vanuit de EER worden doorgegeven.

5) Tijdelijke bulksgewijze verzameling ter ondersteuning van de eerste technische fase van de gerichte verzameling

156. Het EDPB herinnert eraan dat, in het kader van de laatste gezamenlijke evaluatie van het privacyschild, de besprekingen vooral gingen over de interpretatie en toepassing van de aanvullende grond (situatie/scenario) voor bulksgewijze verzameling waarin is voorzien in sectie 2, voetnoot 5, eerste zin van PPD-28, waarin is bepaald dat de in deze sectie opgenomen beperkingen niet van toepassing zijn op SIGINT-gegevens die tijdelijk worden verkregen om gerichte verzameling te vergemakkelijken. De Amerikaanse autoriteiten hebben destijds uitgelegd wat de betekenis is van “SIGINT-gegevens die tijdelijk worden verkregen om gerichte verzameling te vergemakkelijken”. Het EDPB heeft uit deze

¹⁵⁹ Zie met name EO 14086, sectie 2, (c), (iii), (A), (1), (d).

¹⁶⁰ Zie bijvoorbeeld Advies 14/2021 van het EDPB betreffende het ontwerp van uitvoeringsbesluit van de Europese Commissie overeenkomstig Verordening (EU) 2016/679 betreffende de adequate bescherming van persoonsgegevens in het Verenigd Koninkrijk. Vastgesteld op 13 april 2021, punten 4.3.2.1 en 4.3.2.2.

¹⁶¹ EO 14086, sectie 2, (c), (iii), (A), (1), (d).

¹⁶² Zie EHRM (Grote Kamer), Centrum för rättsvisa/Zweden, 25 mei 2021, punt 326.

besprekingen opgemaakt dat deze voetnoot betekent dat gegevens bulksgewijs mogen worden verzameld — en los van de zes beoogde doeleinden — indien zij tijdelijk worden verzameld met het oog op het vaststellen van een identicator voor een bepaald doel. Dit zou dus een extra grond zijn om gegevens bulksgewijs te verzamelen, en in dit geval zouden alleen de algemene beginselen van sectie 1 van PPD-28 nog van toepassing zijn geweest. Zoals hierboven vermeld, was het Hof in het arrest Schrems II van oordeel dat de combinatie van EO 12333 en PPD-28 met betrekking tot de bulksgewijze verzameling “niet op voldoende duidelijke en nauwkeurige wijze de reikwijdte [afbakent] van een dergelijke bulksgewijze verzameling van persoonsgegevens”¹⁶³.

157. Het EDPB merkt op dat in EO 14086 nog steeds een afwijking is opgenomen die een dergelijke bulksgewijze verzameling mogelijk maakt¹⁶⁴; het EDPB is echter verheugd dat deze afwijking in vergelijking met PPD-28 is beperkt en dat in het kader van EO 14086 aanvullende waarborgen worden geboden.
158. Het EDPB begrijpt dat het nieuwe EO 14086 voorziet in waarborgen die van toepassing blijven in het kader van dit soort tijdelijke technische bulksgewijze verzameling, met name de algemene beginselen van noodzakelijkheid en evenredigheid in verband met de gevalideerde inlichtingenprioriteit wanneer gegevens zonder discriminanten worden verkregen voordat gerichte verzameling plaatsvindt (EO 14086, sectie 2, (a)-(b), sectie 2, (c), (i)). Het EDPB gaat er tevens van uit dat een dergelijke bulksgewijze verzameling ter ondersteuning van een daaropvolgende gerichte verzameling van SIGINT ook onderworpen is aan de aanvullende waarborgen waarin wordt voorzien door sectie 2, (c), (iii) en verder¹⁶⁵.
159. Het EDPB herinnert er echter ook aan — zie punt 117 hierboven — dat de definitie van “gevalideerde inlichtingenprioriteit” voorziet in een afwijkende procedure waarbij de CLPO van het Office of the Director of National Intelligence niet betrokken is.
160. Het EDPB merkt echter nog steeds op dat de waarborgen van de sectie betreffende de bulksgewijze verzameling van gegevens niet van toepassing zijn op de tijdelijke bulksgewijze verzameling van gegevens ter ondersteuning van de eerste technische fase van de gerichte verzameling van SIGINT, zoals omschreven in sectie 2, (c), (ii), (D), EO 14086, hetgeen met name betekent dat in deze context bulksgewijze verzamelde gegevens kunnen worden gebruikt voor andere dan de in sectie 2, (c), (ii), genoemde doeleinden. Het EDPB zou graag zien dat in het ontwerpbesluit wordt verduidelijkt voor welke doeleinden in deze context bulksgewijs verzamelde gegevens kunnen worden gebruikt, en dat de in sectie 2, (c), (i), vastgestelde beperkingen voor het verzamelen van SIGINT in het algemeen (namelijk alleen voor de daar genoemde legitieme doeleinden) worden toegepast in het kader van het tijdelijke bulksgewijs verzamelen.
161. Tot slot benadrukt het EDPB ook dat deze afwijking voor tijdelijke bulksgewijze verzameling met het oog op gerichte verzameling en de overige toe te passen waarborgen onduidelijk blijven, met name wat betreft de vraag welke waarborgen van EO 14086 in welk stadium (bulksgewijze verzameling, verdere gerichte verzameling) van toepassing zouden zijn, en verzoekt het EDPB de Commissie deze elementen nader te beoordelen en deze aspecten ook in de praktijk te beoordelen bij de toekomstige gezamenlijke evaluaties.
162. Voorts betreurt het EDPB dat het begrip “tijdelijk” in het EO weliswaar iets gedetailleerder is dan in PPD-28, maar volgens het EDPB nog steeds lijkt te betekenen dat de bulksgewijze verzameling kan

¹⁶³ Arrest Schrems II van het Hof, punt 183.

¹⁶⁴ Zie EO 14086, sectie 2, (c), (ii), D, en ontwerpbesluit, voetnoot 226.

¹⁶⁵ Zie de vorige punten voor nadere elementen over deze bepalingen.

worden voortgezet zolang het doelwit niet geïdentificeerd is. In dit verband herinnert het EDPB aan de noodzaak van duidelijke en precieze regels en benadrukt het ook hier dat deze regels voor de betrokkenen een essentiële waarborg vormen.

163. Tot slot, wat de waarborgen voor bulksgewijze verzameling betreft, blijft het het EDPB zorgen baren dat, ondanks aanvullende waarborgen uit hoofde van EO 14086, nog steeds de mogelijkheid wordt geboden om gegevens bulksgewijs, d.w.z. zonder onderscheid, te verzamelen, zonder essentiële waarborgen zoals voorafgaande toestemming voor het verzamelen van deze gegevens — ook in de afwijkende situatie van tijdelijke technische bulksgewijze verzameling —, mede gelet op de noodzaak van verdere verduidelijking en de geuite bezorgdheid met betrekking tot een strikte doelbinding voor de latere toegang tot de gegevens, duidelijke en strenge regels voor het bewaren van gegevens en striktere waarborgen voor de verspreiding van bulksgewijs verzamelde gegevens, ook in het kader van verdere doorgifte.
164. In het algemeen benadrukt het EDPB dat bovengenoemd arrest van het EHRM een ste meer het belang van alomvattend toezicht door onafhankelijke toezichthoudende autoriteiten aantoonst. Het EDPB benadrukt dat onafhankelijk toezicht in alle stadia van het proces van toegang door de overheid ten behoeve van de nationale veiligheid een belangrijke waarborg is tegen willekeurige surveillancemaatregelen en dus voor de beoordeling van een passend niveau van gegevensbescherming. De garantie van onafhankelijkheid van de toezichthoudende autoriteiten in de zin van artikel 8, lid 3, van het Handvest is bedoeld om een doeltreffend en betrouwbaar toezicht op de naleving van de voorschriften inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens te garanderen. Dit geldt met name in omstandigheden waarin de betrokkene, vanwege de aard van de geheime surveillance, geen toetsing kan aanvragen of vóór of tijdens de uitvoering van de surveillancemaatregel niet rechtstreeks aan een toetsingsprocedure kan deelnemen.
165. Het EDPB herinnert eraan dat hij van mening is dat de beoordeling van de adequaatheid afhangt van alle omstandigheden van het geval, met name van de doeltreffendheid van het toezicht achteraf en de verhaalsmiddelen waarin het rechtskader voorziet.

3.2.2.4 Rechtskader voor het organiseren van specifieke verzameling ten behoeve van de nationale veiligheid door de onderdelen van de inlichtingendiensten binnen en buiten het grondgebied van de VS

166. In zijn arrest Schrems II heeft het Hof met betrekking tot sectie 702 FISA benadrukt dat uit deze tekst “op geen enkele wijze het bestaan van beperkingen van de daarin vervatte bevoegdheid [blijkt] voor de uitvoering van surveillanceprogramma’s met het oog op het verkrijgen van buitenlandse inlichtingen, noch het bestaan van garanties voor in die programma’s potentieel bedoelde niet-Amerikanen”¹⁶⁶. Dit bracht het Hof tot de overweging dat “in die omstandigheden [...] dit artikel geen beschermingsniveau [kan] waarborgen dat in grote lijnen overeenkomt met het niveau dat wordt gewaarborgd door het Handvest [...] volgens welke 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 moet bepalen en duidelijke en nauwkeurige regels moet bevatten die de reikwijdte en de toepassing van de betrokken maatregel bepalen en minimale eisen opleggen”¹⁶⁷.

¹⁶⁶ Arrest Schrems II van het Hof, punt 180.

¹⁶⁷ Arrest Schrems II van het Hof, punt 180.

167. Wat EO 12333 betreft, stelde het Hof vast dat "dit uitvoeringsbevel evenmin rechten verschaft die voor de rechtbanken tegenover de Amerikaanse overheidsdiensten afdwingbaar zijn"¹⁶⁸ en kwam het tot de conclusie dat "[d]eze mogelijkheid om in het kader van op E.O. 12333 gebaseerde surveillanceprogramma's toegang tot gegevens te krijgen tijdens hun doorgifte naar de Verenigde Staten, zonder dat die toegang aan enig gerechtelijk toezicht is onderworpen, [...] hoe dan ook niet op voldoende duidelijke en nauwkeurige wijze de reikwijdte [afbakent] van een dergelijke bulksgewijze verzameling van persoonsgegevens"¹⁶⁹, na de analyse van de voorwaarden waaronder op grond van dit uitvoeringsbevel, in samenhang met PPD-28, bulksgewijze verzameling zou kunnen plaatsvinden.
168. Met betrekking tot deze specifieke gegevensverzamelingsregelingen voorziet EO 14086 nu in nieuwe regels.

3.2.2.4.1 Verzamelen van gegevens ten behoeve van de nationale veiligheid uit hoofde van sectie 702

169. Het EDPB wijst erop dat de bevindingen over sectie 702 FISA¹⁷⁰, namelijk dat in de praktijk ook "niet-Amerikanen" profiteren van de beperkingen op toegang en bewaring die in de minimaliserings- en/of gerichtheidsprocedures van de verschillende diensten worden vereist, omdat de kosten en de moeilijkheid om voor een grote hoeveelheid gegevens informatie over Amerikanen te identificeren en te verwijderen, betekenen dat doorgaans de gehele gegevensreeks wordt behandeld met inachtneming van de strengere Amerikaanse gegevensnormen, in het laatste verslag van de PCLOB werden toegejuicht.
170. Volgens deze bevindingen werkt het programma niet door het bulksgewijs verzamelen van berichten. De door het ODNI uitgegeven statistische transparantieverslagen over 2014 en 2021 bevestigden deze bevinding. Bovendien worden volgens het verslag van de PCLOB opgegeven selectietermen, zoals een e-mailadres of een telefoonnummer, gebruikt om de surveillance te richten.
171. Het EDPB herinnert er echter ook aan dat bij de laatste evaluatie van het privacyschild in het kader van sectie 702 is verduidelijkt dat een "persoon" die als doelwit moet worden geïdentificeerd, kan verwijzen naar verscheidene personen die dezelfde identifier gebruiken, mits al deze personen niet-Amerikanen zijn en voldoen aan de toepasselijke criteria om als doelwit te worden aangemerkt. Ook herinnert het EDPB eraan dat tijdens de derde jaarlijkse gezamenlijke evaluatie van het privacyschild in 2019 is opgeroepen tot verdere verduidelijking in het kader van het Upstream-programma om uit te sluiten dat massale en ongedifferentieerde toegang tot persoonsgegevens van niet-Amerikanen plaatsvindt¹⁷¹.
172. Bovendien wijst het EDPB erop dat het verzamelen op grond van sectie 702 FISA wordt gerechtvaardigd door de uitspraak dat het verkrijgen van buitenlandse inlichtingen een belangrijk doel is en dat dit nog steeds enige onzekerheid laat bestaan over de doelbinding en de noodzakelijkheid ervan. Het EDPB merkt echter op dat volgens EO 14086, sectie 2, (a), (A) en (B), activiteiten op het gebied van SIGINT alleen mogen worden verricht nadat is vastgesteld dat de activiteiten noodzakelijk zijn om een gevalideerde prioriteit te bevorderen en alleen in de mate en op een wijze die evenredig is aan die prioriteit en dat zij zo gericht mogelijk moeten plaatsvinden om de gevalideerde prioriteit te bevorderen, waarbij terdege rekening wordt gehouden met relevante factoren zoals de indringendheid van de verzameling en de gevoeligheid van de gegevens, en geen onevenredige gevolgen mogen hebben voor de privacy en de burgerlijke vrijheden. Het EDPB verwacht nog verdere

¹⁶⁸ Arrest Schrems II van het Hof, punt 182.

¹⁶⁹ Arrest Schrems II van het Hof, punt 183.

¹⁷⁰ Zie het verslag van de PCLOB over het surveillanceprogramma uit hoofde van sectie 702 FISA, blz. 100.

¹⁷¹ Derde jaarlijkse gezamenlijke evaluatieverslag, blz. 17, punt 83.

verduidelijkingen over de manier waarop dit concreet zal worden uitgevoerd en operationeel gemaakt, ook in het kader van de toepassing van sectie 702 FISA.

173. In dit verband heeft het EDPB, bij gebrek aan rechtstreekse toegang tot deze informatie, verzocht om een onafhankelijke beoordeling van de noodzakelijkheid en de evenredigheid van de definitie van “doelwitten” en van het begrip “buitenlandse inlichtingen” in het kader van sectie 702 FISA (ook in de context van het Upstream-programma) na de verlenging ervan. Het EDPB is van mening dat zijn eerdere verzoek om verdere onafhankelijke beoordeling van het proces in verband met de toepassing van selectietermen in specifieke gevallen (“tasking of selectors”) en om verdere verduidelijking in de context van het Upstream-programma relevant is. Rekening houdend met het nieuwe EO 14086 verzoekt het EDPB derhalve om aanvullende informatie opdat hij ook in dit verband zou kunnen beoordelen en controleren hoe en in welke mate de nieuw ingevoerde beginselen van noodzakelijkheid en evenredigheid in de praktijk zullen worden toegepast. Het EDPB verwacht dat dit ook in het kader van toekomstige gezamenlijke evaluaties zal worden beoordeeld.
174. Het EDPB is verheugd dat de volledig operationele Privacy and Civil Liberties Oversight Board (PCLOB), als onafhankelijk toezichtsorgaan, heeft besloten een toezichtsproject uit te voeren om het surveillanceprogramma te onderzoeken dat de uitvoerende macht gebruikt overeenkomstig sectie 702 van de Foreign Intelligence Surveillance Act (FISA), vooruitlopend op de vervaldatum van december 2023 voor sectie 702 en de komende openbare debatten en besprekingen in het Congres over de nieuwe goedkeuring ervan¹⁷². Het EDPB juicht ook toe dat de evaluatie betrekking heeft op geselecteerde aandachtsgebieden voor onderzoek, waaronder, maar niet noodzakelijkerwijs beperkt tot, het opvragen van gegevens van Amerikanen die in het kader van sectie 702 zijn verzameld, en het verzamelen van gegevens in het kader van “Upstream” overeenkomstig sectie 702¹⁷³ en dat deze tevens een toetsing omvat van de vroegere en verwachte waarde en doeltreffendheid van het programma, alsmede van de adequaatheid van de bestaande waarborgen inzake privacy en burgerlijke vrijheden¹⁷⁴. Het EDPB benadrukt derhalve dat toegang tot de bevindingen van de PCLOB in dit verslag over sectie 702 noodzakelijk zou zijn om de in het kader van dit surveillanceprogramma geboden en toegepaste waarborgen voor de privacy adequaat en volledig te beoordelen.
175. Rekening houdend met het nieuwe EO 14086 verzoekt het EDPB bovendien om aanvullende informatie opdat hij ook zou kunnen beoordelen en controleren hoe en in welke mate de nieuw ingevoerde beginselen van noodzakelijkheid en evenredigheid, alsmede de andere in deze tekst genoemde waarborgen in dit kader in de praktijk zullen worden toegepast.

3.2.2.4.2 Verzamelen van gegevens ten behoeve van de nationale veiligheid uit hoofde van Executive Order 12333

176. Zoals het Hof in zijn arrest Schrems II heeft erkend, mag de analyse van de wetgeving van het derde land waarvoor de adequaatheid wordt overwogen, niet beperkt blijven tot de wetten en praktijken die surveillance binnen de fysieke grenzen van dat land toestaan, maar moet zij ook een analyse omvatten van de rechtsgronden in de wetgeving van dat derde land die het mogelijk maken buiten zijn grondgebied surveillance te voeren wat EU-gegevens betreft. Noodzakelijke beperkingen van de

¹⁷² Zie [NOTICE OF THE PCLOB OVERSIGHT PROJECT EXAMINING SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT \(FISA\)](#).

¹⁷³ Zie hierboven.

¹⁷⁴ Zie hierboven.

toegang van de overheid tot gegevens moeten zich uitstrekken tot persoonsgegevens “in doorvoer” naar het land waarvoor de adequaatheid wordt erkend.

177. Het EDPB verwelkomt het algemene openbare verslag van de PCLOB over Executive Order 12333 dat in april 2021 is uitgebracht, maar merkt op dat dit verslag algemeen blijft omdat de meeste bevindingen gerubriceerd zijn.
178. In dit verband benadrukt het EDPB, gezien de onzekerheid en het gebrek aan duidelijkheid over de toepassing van EO 12333 en het belang van verduidelijking van de toepassing ervan in het licht van het nieuwe EO 14086, nogmaals het belang van de verwachte verslagen van de PCLOB over deze tekst¹⁷⁵. Het EDPB begrijpt echter dat de inhoud daarvan waarschijnlijk grotendeels gerubriceerd zal blijven, zodat noch het publiek, noch het EDPB verdere informatie zal krijgen over de concrete werking van EO 12333 en over de noodzakelijkheid en evenredigheid ervan.
179. Het EDPB zou het daarom bijzonder toejuichen indien het verslag van de PCLOB over de toepassing van EO 14086 niet gerubriceerd maar volledig toegankelijk zou zijn zodra het voltooid is, met inbegrip van de delen waarin wordt beoordeeld hoe de waarborgen van EO 14086 zullen worden toegepast op het verzamelen van gegevens uit hoofde van EO 12333. Het EDPB verzoekt de Commissie tevens om in het kader van de toekomstige gezamenlijke evaluaties bijzondere aandacht aan dit punt te besteden.
180. In het algemeen zou het EDPB, met betrekking tot de verschillende rechtsinstrumenten die de Amerikaanse inlichtingendiensten in het rechtskader van de Verenigde Staten de mogelijkheid bieden om gegevens te verzamelen en verder te raadplegen en te verwerken, graag opheldering krijgen over de wisselwerking daarvan met het nieuwe EO 14086 en verwacht hij de verzekering dat de eerdere bezwaren die het EDPB in eerdere adviezen daarover heeft geuit, worden weggenomen door de vaststelling van deze nieuwe waarborgen.
181. Het EDPB verzoekt de Commissie tevens om in het kader van toekomstige gezamenlijke evaluaties bijzondere aandacht aan deze aspecten te besteden.

3.2.2.4.3 Verslag van de PCLOB

182. Het EDPB is verheugd dat EO 14086 ook bepaalt dat de PCLOB een verslag over de uitvoering van het EO moet opstellen. Het EDPB benadrukt dat dit verslag een beoordeling moet bevatten van deze specifieke door het EO geboden mogelijkheid om gegevens te verzamelen, zowel voor de genoemde doeleinden voor gerichte verzameling, als voor bulksgewijze verzameling, ook om technische redenen, teneinde een beter inzicht te krijgen in de kernbegrippen van EO 14086 en de wijze waarop deze in de praktijk worden uitgelegd en toegepast in de verschillende toezichtsprogramma's. Dit verslag zou ook nodig zijn om te beoordelen hoe het EO zal worden uitgevoerd in de interne procedures en het beleid van de onderdelen van de inlichtingendiensten.

¹⁷⁵ Het algemene verslag over EO 12333 is grotendeels gerubriceerd gebleven — alleen een korte openbare versie is bekendgemaakt, evenals het verslag en de aanbevelingen over terrorismebestrijding door de CIA overeenkomstig EO 12333, die eveneens slechts gedeeltelijk gederubriceerd zijn.

3.2.3 Garantie C — Toezicht

3.2.3.1 Inleiding

183. De Amerikaanse inlichtingenactiviteiten zijn onderworpen aan een meerlagig toezichtproces. De toezichtstructuur in de VS kan worden onderverdeeld in intern en extern toezicht. Alle onderdelen van de inlichtingendiensten hebben functionarissen voor toezicht en naleving, die periodiek toezicht houden op de activiteiten op het gebied van SIGINT, waaronder functionarissen voor privacy en burgerlijke vrijheden (Privacy and Civil Liberties Officers) en inspecteurs-generaal (Inspectors General). Daarnaast zijn er externe toezichtsorganen, zoals de Privacy and Civil Liberties Oversight Board (PCLOB) en de Intelligence Oversight Board.
184. Het EDPB herinnert eraan dat inmenging plaatsvindt op het moment dat de gegevens worden verzameld, maar ook op het moment dat een overheidsinstantie toegang krijgt tot de gegevens voor verdere verwerking. Het EHRM heeft herhaaldelijk gespecificeerd dat elke aantasting van het recht op privacy en gegevensbescherming onderworpen moet zijn aan een doeltreffend, onafhankelijk en onpartijdig toezichtstelsel, dat ofwel door een rechter, ofwel door een ander onafhankelijk orgaan¹⁷⁶ (bijvoorbeeld een administratieve autoriteit of een parlementair orgaan) moet worden ingesteld.
185. Het EHRM heeft weliswaar zijn voorkeur uitgesproken voor een rechter die verantwoordelijk is voor het toezicht, maar heeft niet uitgesloten dat een ander orgaan verantwoordelijk kan zijn, mits deze instantie voldoende onafhankelijk is van de uitvoerende macht¹⁷⁷ en van de autoriteiten die het toezicht uitoefenen, en over voldoende bevoegdheden en bekwaamheid beschikt om een doeltreffende en voortdurende controle uit te oefenen¹⁷⁸.
186. Het EHRM voegde daaraan toe dat de wijze van benoeming en de rechtspositie van de leden van het toezichthoudend orgaan¹⁷⁹ bij de beoordeling van de onafhankelijkheid in aanmerking moeten worden genomen.
187. Het EHRM stelt ook dat moet worden onderzocht of de activiteiten van het toezichthoudend orgaan aan publieke toetsing kunnen worden onderworpen. Dit zou bijvoorbeeld kunnen worden bereikt wanneer het toezichthoudend orgaan jaarlijks verslag uitbrengt aan de regering, respectievelijk de openbare verslagen aan het parlement worden voorgelegd en door het parlement worden besproken¹⁸⁰.
188. Het onafhankelijke toezicht op de uitvoering van surveillancemaatregelen is ook door het Hof in aanmerking genomen in het arrest Schrems II: “[...] de door de FISC uitgeoefende controle [heeft] dus tot doel na te gaan of deze surveillanceprogramma’s beantwoorden aan de doelstelling om buitenlandse inlichtingen te verkrijgen maar die controle [betreft] niet de vraag of “natuurlijke personen het juiste doelwit zijn om buitenlandse inlichtingen te verwerven”. ”¹⁸¹

¹⁷⁶ EHRM, zaak Klass e.a./Duitsland, 6 september 1978 (hierna het “EHRM-arrest Klass”), punten 17 en 51.

¹⁷⁷ EHRM-arrest Zakharov, punt 258; EHRM, Iordachi e.a./Moldavië, 10 februari 2009, punten 40 en 51; EHRM, Dumitru Popescu/Roemenië, 26 april 2007, punten 70-73.

¹⁷⁸ EHRM-arrest Klass, punt 56.

¹⁷⁹ EHRM-arrest Zakharov, punt 278.

¹⁸⁰ EHRM-arrest Zakharov, punt 283; EHRM, L./Noorwegen, 9 juni 1990; EHRM, Kennedy/Verenigd Koninkrijk, 18 mei 2010, punt 166.

¹⁸¹ Arrest Schrems II van het Hof, punt 179.

3.2.3.2 Intern toezicht

3.2.3.2.1 Inspecteurs-generaal

189. Het EDPB erkent dat aan de inspecteurs-generaal een breed scala aan bevoegdheden is toegekend, die nodig zijn voor het toezicht op de inlichtingenactiviteiten. De inspecteurs-generaal hebben met name toegang tot alle informatie die nodig is om te beoordelen of de werkzaamheden van de diensten in het algemeen in overeenstemming zijn met de wetgeving, met inbegrip van, maar niet beperkt tot de wetgeving inzake privacy en gegevensbescherming, en kunnen in verband met het onderzoek van de inspecteurs-generaal eenieder dagvaarden en onder eed laten getuigen.
190. Op basis van het bovenstaande is het EDPB van mening dat de inspecteurs-generaal in het algemeen over uitgebreide onderzoeksbevoegdheden beschikken. Zij hebben echter geen bindende corrigerende bevoegdheden en doen alleen niet-bindende aanbevelingen¹⁸².
191. Het EDPB erkent dat het de inspecteurs-generaal in beginsel niet wordt belet of verboden een audit of onderzoek in te stellen, uit te voeren of af te ronden, noch in de loop van een audit of onderzoek een dagvaarding uit te vaardigen¹⁸³. In dit verband merkt het EDPB evenwel op dat de inspecteurs-generaal onder het gezag, de leiding en het toezicht staan van het respectieve hoofd van het ministerie, dat hen de toegang tot informatie, het verrichten van een onderzoek en onder meer het uitvaardigen van een dagvaarding kan verbieden in gevallen waarin het hoofd van het ministerie bepaalt dat een dergelijk verbod noodzakelijk is om nationale belangen te beschermen. Het hoofd van het ministerie moet echter de bevoegde commissies van het Amerikaanse Congres in kennis stellen van de uitoefening van deze bevoegdheid¹⁸⁴.
192. Het EDPB merkt op dat inspecteurs-generaal alleen kunnen worden ontslagen door de Amerikaanse president, die het Congres op de hoogte moet stellen van de redenen voor dat ontslag.
193. Het EDPB merkt op dat er sinds de adviezen van de Groep gegevensbescherming artikel 29 en vervolgens het EDPB geen significante wijzigingen in het interne toezichtmechanisme zijn aangebracht. Het EDPB concludeert dan ook, in overeenstemming met Advies 01/2016 van de Groep gegevensbescherming artikel 29¹⁸⁵ dat er in het algemeen voldoende interne toezichtmechanismen aanwezig zijn.

3.2.3.3 Extern toezicht

194. Het EDPB merkt op dat naast de hieronder genoemde organen diverse andere organen binnen de Amerikaanse regering toezicht houden op de activiteiten van de Amerikaanse inlichtingendiensten, zoals de Intelligence Oversight Board (IOB) of de commissies van het Congres. Deze commissies kunnen hun eigen onderzoeken uitvoeren en verslagen opstellen.

¹⁸² Ontwerpbesluit, overweging 105.

¹⁸³ Inspector General Act of 1978, § 3 (a).

¹⁸⁴ Zie bv. Inspector General Act of 1978, § 8 (voor het ministerie van Defensie); § 8E (voor het ministerie van Justitie), § 8G (d)(2)(A),(B) (voor de NSA); 50. U.S.C. § 403q, (b) (voor de CIA); Intelligence Authorization Act For Fiscal Year 2010, sectie 405(f) (voor de inlichtingendiensten).

¹⁸⁵ Advies 01/2016 van de Groep gegevensbescherming artikel 29.

3.2.3.3.1 Raad van toezicht op de privacy en de burgerlijke vrijheden (Privacy and Civil Liberties Oversight Board, “PCLOB”)

195. Het EDPB erkent de uitgebreide toezichthoudende rol van de PCLOB met betrekking tot het nieuwe verhaalmechanisme en de uitvoering van EO 14086.
196. Ten eerste omvatten zijn nieuwe taken overleg met de minister van Justitie over de benoeming van de rechters van de DPRC en de bijzondere juristen (*special advocates*). Ten tweede zal de PCLOB het verhaalmechanisme, d.w.z. de verwerking van in aanmerking komende klachten door het verhaalmechanisme, jaarlijks evalueren. In deze evaluatie wordt nagegaan of de CLPO en de Data Protection Review Court in aanmerking komende klachten tijdig verwerken, volledige toegang krijgen tot de noodzakelijke informatie en handelen in overeenstemming met EO 14086, alsmede of de inlichtingendiensten de vaststellingen van de CLPO en de DPRC naleven.
197. Voorts moet de PCLOB worden geraadpleegd terwijl de inlichtingendiensten hun interne beleidsmaatregelen en procedures bijwerken om uitvoering te geven aan EO 14086. Bovendien zal de PCLOB de bijgewerkte beleidsmaatregelen en procedures evalueren en nagaan of zij in overeenstemming zijn met EO 14086¹⁸⁶. Hoewel de bevindingen van de PCLOB niet bindend zijn in strikte zin, is het hoofd van elk onderdeel van de inlichtingendiensten verplicht alle aanbevelingen in een dergelijke evaluatie zorgvuldig te overwegen en uit te voeren of anderszins aan te pakken, in overeenstemming met de toepasselijke wetgeving¹⁸⁷. Het EDPB verzoekt de Commissie bij toekomstige evaluaties, indien het ontwerpbesluit wordt vastgesteld, bijzondere aandacht te besteden aan de vraag of en hoe de aanbevelingen van de PCLOB op het niveau van de diensten zijn uitgevoerd.
198. Het EDPB herinnert eraan dat de PCLOB, aangezien hij onafhankelijk is, wordt “aangemoedigd” om na te gaan of de in EO 14086 vastgestelde waarborgen naar behoren in aanmerking zijn genomen en of de inlichtingendiensten de vereisten van het verhaalmechanisme volledig hebben nageleefd. De PCLOB is daartoe echter niet verplicht. Het EDPB heeft echter begrepen dat de PCLOB in zijn aanvullende toelichting aan het EDPB en in het openbaar¹⁸⁸ heeft verklaard dat hij de in EO 14086 bedoelde rol op zich zal nemen.
199. Voorts juicht het EDPB toe dat het de bedoeling is de resultaten van de verslagen van de PCLOB openbaar te maken. Rekening houdend met het feit dat de verschillende organen binnen het verhaalmechanisme en die van de inlichtingendiensten in beginsel de aanbevelingen in de verslagen van de PCLOB moeten uitvoeren of anderszins moeten aanpakken, erkent het EDPB dat deze aanbevelingen een belangrijke rol spelen bij het waarborgen van de privacy.

¹⁸⁶ EO 14086, sectie 2, (c), (iv) en sectie 2, (c), (v).

¹⁸⁷ EO 14086, sectie 2, (c), (v), (B).

¹⁸⁸ [https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20\(FINAL\).pdf](https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf)

200. Het EDPB merkt op dat de toegang van de PCLOB tot informatie wordt beperkt indien de Amerikaanse president toestemming geeft voor het uitvoeren van “geheime acties”¹⁸⁹ door ministeries, diensten of entiteiten van de regering van de Verenigde Staten¹⁹⁰.
201. Overeenkomstig zijn eerdere adviezen beschouwt het EDPB de PCLOB als een onafhankelijk orgaan, waarvan de aanbevelingen een belangrijke bijdrage zijn geweest tot hervormingen in de VS en waarvan de verslagen een bijzonder nuttige bron zijn geweest om inzicht te krijgen in de werking van de verschillende surveillanceprogramma’s, als een essentieel onderdeel van de toezichtstructuur.
202. In zijn derde jaarlijkse gezamenlijke evaluatie van het vroegere EU-VS-privacyschild betreunde het EDPB echter dat de PCLOB het EDPB slechts dezelfde informatie verstrekke als het grote publiek. Voorts viel het te betreuren dat de PCLOB geen verdere verslagen over PPD-28 heeft uitgebracht als vervolg op zijn eerste verslag, teneinde aanvullende elementen te verstrekken over de wijze waarop de waarborgen van PPD-28 worden toegepast, alsmede een algemeen geactualiseerd verslag over sectie 702 FISA.
203. Het EDPB is dan ook ingenomen met de aankondiging van de PCLOB aan het EDPB dat de publicatie van een vervolgverslag over sectie 702 FISA in de nabije toekomst mag worden verwacht. Voorts is het EDPB tevreden dat de PCLOB zijn toezegging heeft aangekondigd om zijn verslagen betreffende EO 14086 openbaar te maken. Het EDPB herinnert er echter aan dat de vrijgave van niet-gerubriceerde verslagen door de Amerikaanse wetgeving wordt geregeld en moet worden gecoördineerd met de inlichtingendiensten en dat de PCLOB niet op eigen houtje kan beslissen.
204. Indien het ontwerpbesluit wordt vastgesteld, wijst het EDPB er derhalve op dat bij toekomstige evaluaties van het EU-VS-kader voor gegevensbescherming de EDPB-deskundigen met een veiligheidsmachtiging aanvullende documenten moeten kunnen bestuderen en aanvullende gerubriceerde elementen moeten kunnen bespreken indien dit nodig is om de informatie in de verslagen naar behoren te kunnen beoordelen, rekening houdend met relevante nationale veiligheidsbelangen en toepasselijke privacybeschermingen.
205. Het EDPB is verheugd over de onafhankelijkheid van de PCLOB en het toezicht op de nationale inlichtingendiensten, die de aanbevelingen van de PCLOB moeten opvolgen of anderszins moeten aanpakken, hetgeen zal worden aangegeven in het verslag van de PCLOB aan het Amerikaanse Congres.
206. Rekening houdend met de vereisten van het EHRM inzake openbare controle¹⁹¹, namelijk dat de verslagen van een toezichthoudend orgaan aan het parlement moeten worden voorgelegd en door het parlement moeten worden besproken, acht het EDPB het voldoende dat de PCLOB zijn verslagen ten minste halfjaarlijks voorlegt aan de president van de VS en in het bijzonder aan de Committeees

¹⁸⁹ Volgens 50 U.S.C. § 3093, (e), (1), betekent de term “geheime actie” een activiteit of activiteiten van de regering van de Verenigde Staten om politieke, economische of militaire omstandigheden in het buitenland te beïnvloeden, waarbij het de bedoeling is dat de rol van de regering van de Verenigde Staten niet openbaar wordt gemaakt of erkend, maar omvat de term niet (1) activiteiten waarvan het hoofddoel het verwerven van inlichtingen is, traditionele contraspionageactiviteiten [...].

¹⁹⁰ 42 U.S.C. § 2000ee, (g), (5); 50 U.S. Code § 3093, (a).

¹⁹¹ EHRM-arrest Zakharov, punt 283; EHRM, L./Noorwegen, 9 juni 1990; EHRM, Kennedy/Verenigd Koninkrijk, 18 mei 2010, punt 166.

(commissies) van het Congres (de Senaat en het Huis van Afgevaardigden)¹⁹², die de parlementaire organen van de VS zijn.

3.2.3.3.2 *Foreign Intelligence Surveillance Court (FISC)*

207. De Foreign Intelligence Surveillance Court is verantwoordelijk voor het toezicht op de verzameling van persoonsgegevens overeenkomstig sectie 702 FISA¹⁹³ en tegen de beslissingen van de FISC kan beroep worden aangetekend bij de Foreign Intelligence Surveillance Court of Review (FISCR).
208. De FISC houdt toezicht op het certificeringsproces voor het verzamelen van buitenlandse inlichtingen overeenkomstig sectie 702 FISA en geeft toestemming voor elektronische surveillance, fysieke doorzoeken en andere onderzoeksmaatregelen voor buitenlandse inlichtingen¹⁹⁴. De FISC machtigt ook de procedures om het doelwit te specificeren, de minimaliseringsprocedures en de procedures voor het doorzoeken van de certificaten, die juridisch bindend zijn voor de Amerikaanse inlichtingendiensten¹⁹⁵. Indien de FISC vaststelt dat niet aan de vereisten is voldaan, kan hij de certificering geheel of gedeeltelijk afwijzen en eisen dat de procedures worden gewijzigd.
209. Indien schendingen van de gerichtheidsprocedures worden vastgesteld, kan de FISC de betrokken inlichtingendienst gelasten corrigerende maatregelen te nemen¹⁹⁶. Hierbij kan het gaan om individuele en structurele maatregelen, zoals het beëindigen van de gegevensverwerking en het wissen van onrechtmatig verkregen gegevens, tot een verandering in de praktijk van het verzamelen, maar ook richtsnoeren voor en opleiding van personeel.
210. Het EDPB erkent dat EO 14086 bepaalt dat de CLPO en de DPRCSchendingen moeten rapporteren aan de Assistant Attorney General for National Security (viceminister van Justitie voor de nationale veiligheid), die deze schendingen moet rapporteren aan de FISC¹⁹⁷.
211. Zoals het Hof in zijn arrest Schrems II heeft opgemerkt, geeft de FISC geen toestemming voor individuele surveillancemaatregelen; de FISC geeft in plaats daarvan toestemming voor surveillanceprogramma's¹⁹⁸. Het EDPB blijft dan ook bezorgd dat de FISC geen doeltreffend rechterlijk toezicht uitoefent op het specificeren van niet-Amerikaanse doelwitten, hetgeen met het nieuwe EO 14086 niet lijkt te zijn opgelost.
212. Met betrekking tot de voorafgaande onafhankelijke toestemming¹⁹⁹ voor surveillance uit hoofde van sectie 702 FISA betreurt het EDPB dat, zoals het EDPB heeft begrepen uit het ontwerpbesluit²⁰⁰ en de door de Amerikaanse regering verstrekte uitleg, de FISC niet gebonden lijkt te zijn aan de aanvullende waarborgen van EO 14086 bij het certificeren van de programma's die het specificeren van niet-Amerikaanse doelwitten toestaan. Naar het oordeel van het EDPB moet in dit verband niettemin rekening worden gehouden met de in dit EO vervatte aanvullende waarborgen. Het EDPB herinnert eraan dat verslagen van de PCLOB bijzonder nuttig zouden zijn om te beoordelen hoe de waarborgen

¹⁹² 42 U.S.C. § 2000ee, (e).

¹⁹³ 50 U.S.C. 1881 (a).

¹⁹⁴ www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court

¹⁹⁵ 50 U.S.C. 1881a, (i).

¹⁹⁶ 50 U.S.C. § 1803, (h).

¹⁹⁷ EO 14086, sectie 3, (c), (i), (D); EO 14086, sectie 3, (d), (i), (F).

¹⁹⁸ Arrest Schrems II van het Hof, punt 179.

¹⁹⁹ Wat betreft het bulksgewijs verzamelen van gegevens krachtens EO 12333, waarvoor de FISC niet bevoegd is, is het EDPB bezorgd dat er geen voorafgaande toestemmingsprocedure bestaat voor het bulksgewijs verzamelen van gegevens (zie ook waarborg B).

²⁰⁰ Ontwerpbesluit, overweging 165.

van EO 14086 zullen worden uitgevoerd en hoe deze waarborgen worden toegepast wanneer gegevens worden verzameld uit hoofde van sectie 702 FISA.

3.2.4 Garantie D — Personen moeten over doeltreffende voorzieningen in rechte beschikken

213. Het EDPB herinnert eraan dat effectieve en afdwingbare rechten van personen van fundamenteel belang zijn voor het vinden van een passend niveau van gegevensbescherming in een derde land. De betrokkenen moeten over doeltreffende voorzieningen in rechte beschikken om hun rechten te doen gelden wanneer zij menen dat deze niet worden of zijn geëerbiedigd. Het Hof heeft in zijn arresten Schrems I en II het volgende verklaard: “Evenzeer eerbiedigt een regeling die niet in enige beroepsmogelijkheid voor de justitiabele voorziet om toegang tot de hem betreffende persoonsgegevens te verkrijgen, of rectificatie of verwijdering van die gegevens, de wezenlijke inhoud van het grondrecht op een effectieve voorziening in rechte zoals neergelegd in artikel 47 van het Handvest niet.”²⁰¹
214. Het Amerikaanse systeem van voorzieningen in rechte bevat een belangrijke beperking die het zeer moeilijk maakt om bij gewone rechtbanken een rechtszaak aan te spannen tegen surveillancemaatregelen van de Amerikaanse regering. De Amerikaanse grondwet vereist dat een persoon kan aantonen dat hij belang heeft bij het aanhangig maken van een procedure, d.w.z. dat hij een concrete, specifieke en reële of dreigende schade moet aantonen²⁰². In gevallen van surveillance lijkt dit vereiste teniet te worden gedaan doordat natuurlijke personen die onderworpen zijn aan surveillance, hiervan niet in kennis worden gesteld, zelfs nadat deze maatregelen zijn beëindigd.
215. In dit verband is het EDPB verheugd dat EO 14086 voorziet in een specifiek verhaalmechanisme voor de behandeling en oplossing van klachten van niet-Amerikanen over Amerikaanse SIGINT-activiteiten. In dit nieuwe mechanisme is het vereiste inzake het aantonen van dit belang bij het aanhangig maken van een procedure niet van toepassing: volgens sectie 4, (k), (ii), EO 14086 hoeft de eiser niet aan te tonen dat zijn gegevens daadwerkelijk het voorwerp zijn geweest van Amerikaanse SIGINT. De betrokkenen kunnen zich dus beroepen op de waarborgen waarin EO 14086 voorziet, met inbegrip van die waarin andere relevante wetten en bepalingen als bedoeld in sectie 4, (d), (iii), EO 14086 voorzien²⁰³. In dit opzicht voegt het nieuwe mechanisme een verhaalsmogelijkheid toe die anders niet zou bestaan.
216. Het nieuwe mechanisme bestaat uit twee niveaus: op het eerste niveau kunnen natuurlijke personen een klacht indienen bij de Civil Liberties Protection Officer van het Office of the Director of National Intelligence (CLPO). Op het tweede niveau kunnen natuurlijke personen tegen het besluit van de CLPO in beroep gaan bij een nieuw opgericht orgaan, de zogeheten Data Protection Review Court (DPRC). De volgende punten hebben vooral betrekking op het tweede niveau van het verhaalmechanisme. Het EDPB is van mening dat de CLPO, als waarnemend overheidsfunctionaris, niet over een voldoende mate van onafhankelijkheid van de uitvoerende macht beschikt en dus zelf niet adequaat kan voldoen aan de vereisten die voortvloeien uit artikel 47 van het Handvest. Deze beoordeling is herhaaldelijk door de Commissie bevestigd.

²⁰¹ Arrest Schrems I van het Hof, punt 95; arrest Schrems II van het Hof, punt 187.

²⁰² Clapper/Amnesty International USA, 568 U.S. 398 (2013) II., blz. 10.

²⁰³ EO 14086, sectie 5, (h), creëert uitdrukkelijk een recht voor betrokkenen om klachten in te dienen overeenkomstig het verhaalmechanisme.

3.2.4.1 Kan de oprichting van de DPRC op basis van een Executive Order op zich volstaan?

217. De DPRC is geen gewone rechterlijke instantie die door het Congres is ingesteld krachtens artikel III van de Amerikaanse grondwet, maar is gebaseerd op een Executive Order van de Amerikaanse president. Hoewel het EDPB zich bewust is van en in het algemeen ingenomen is met de achterliggende overweging, namelijk het vermijden van het vereiste van belang bij het aanhangig maken van een procedure (zie ook punt 215), roept dit een fundamentele vraag op: kan een dergelijk verhaalmechanisme (überhaupt) voldoen aan de vereisten van artikel 47 van het Handvest? Volgens deze bepaling heeft eenieder wiens door het recht van de Unie gewaarborgde rechten en vrijheden zijn geschonden, recht op een doeltreffende voorziening in rechte voor een gerecht dat vooraf bij wet is ingesteld.
218. Terwijl in de Engelse formulering van artikel 47 van het Handvest sprake is van een “tribunal”, wordt in andere taalversies de voorkeur gegeven aan de term “court”²⁰⁴. In Schrems II heeft het Hof herhaald dat “de justitiabelen moeten beschikken over de mogelijkheid om voor een onafhankelijk en onpartijdig gerecht rechtsmiddelen aan te wenden teneinde toegang te krijgen tot hun persoonsgegevens of rectificatie of verwijdering van dergelijke gegevens te verkrijgen”²⁰⁵. In dezelfde context van de beoordeling van de adequaatheid van het niveau van gegevensbescherming is het Hof evenwel van oordeel dat een doeltreffende rechterlijke bescherming tegen dergelijke inmenging niet alleen kan worden gewaarborgd door een gerecht, maar ook door een orgaan dat waarborgen biedt die in wezen gelijkwaardig zijn aan die welke door artikel 47 van het Handvest worden geëist²⁰⁶. Evenzo bepaalt het EVRM dat eenieder wiens rechten en vrijheden zijn geschonden, beschikt over een doeltreffende voorziening in rechte voor een nationale autoriteit²⁰⁷, die, volgens de vaste rechtspraak van het EHRM, niet noodzakelijk een gerechtelijke autoriteit hoeft te zijn²⁰⁸. Veeleer zijn de bevoegdheden en de procedurele waarborgen waarover een autoriteit beschikt, met name de vraag of zij onafhankelijk is van de uitvoerende macht en het eerlijke verloop van de procedure waarborgt, van belang voor de beoordeling van de doeltreffendheid van de voorziening in rechte voor die autoriteit²⁰⁹. Blijkbaar baseren beide hoven hun beoordeling niet op louter formalistische criteria, maar beschouwen zij de materiële waarborgen als doorslaggevend.
219. In Schrems II heeft het Hof bijzondere aandacht besteed aan de doeltreffende voorziening in rechte op het gebied van toegang tot persoonsgegevens voor de nationale veiligheid. Het EDPB neemt er kennis van dat het Hof daarbij echter niet is ingegaan op het begrip “dat vooraf bij wet is ingesteld” van artikel 47 van het Handvest, ook al was het mechanisme van de privacy-schildombudsman evenmin gebaseerd op Amerikaanse wetgeving. In plaats van deze kwestie te behandelen, heeft het Hof verschillende aspecten voor de adequaatheidstoets beoordeeld, zoals het ontbreken van corrigerende bevoegdheden. Het arrest Schrems II biedt dus geen houvast voor de beoordeling van het begrip “dat vooraf bij wet is ingesteld” overeenkomstig artikel 47 van het Handvest. Er zijn echter andere arresten waarin het Hof zich over deze kwestie heeft uitgelaten. Onder verwijzing naar de vaste rechtspraak van het EHRM ter zake heeft het Hof in de zaken C-487/19 en C-132/20 in herinnering gebracht dat de invoering van het begrip “dat vooraf bij wet is ingesteld” tot doel heeft te voorkomen dat de organisatie van de rechterlijke macht in een democratische samenleving wordt overgelaten aan de

²⁰⁴ Bijvoorbeeld “Gericht” in de Duitse taalversie.

²⁰⁵ Arrest Schrems II van het Hof, punt 194.

²⁰⁶ Arrest Schrems II van het Hof, punt 197.

²⁰⁷ Artikel 13 EVRM.

²⁰⁸ EHRM, arrest Klass, punt 67; EHRM-arrest Big Brother Watch, punt 359.

²⁰⁹ EHRM, arrest Klass, punt 67; EHRM-arrest Big Brother Watch, punt 359.

uitvoerende macht, maar ervoor te zorgen dat deze aangelegenheid wordt geregeld bij een wet die door de wetgevende macht is vastgesteld in overeenstemming met de regels voor de uitoefening van haar bevoegdheid²¹⁰. Zoals uit deze verklaring blijkt, hangt het recht op een vooraf bij wet ingesteld gerecht zeer nauw samen met de waarborg van onafhankelijkheid.

220. Tegen deze achtergrond concludeert het EDPB dat, in het kader van de beoordeling van de adequaatheid van het beschermingsniveau, het specifieke verhaalmechanisme dat bij EO 14086 in het leven is geroepen, in tegenstelling tot het verhaalmechanisme bij de rechterlijke instanties die zijn ingesteld krachtens artikel III van de Amerikaanse grondwet, op zich niet ontoereikend is. De analyse van het beschermingsniveau in dit verband hangt af van de vraag of de in EO 14086 geboden en door het decreet van de Attorney General aangevulde waarborgen de onafhankelijkheid van de DPRC ten opzichte van de andere machten voldoende waarborgen.
221. De Commissie moet voortdurend nagaan of de regels van EO 14086 en de aanvullende bepalingen daarvan, met name die ter bevordering van de onafhankelijkheid van de DPRC, volledig worden uitgevoerd en in de praktijk doeltreffend functioneren. Bovendien moeten eventuele wijzigingen van het kader zorgvuldig worden bekeken op de gevolgen voor de beoordeling door de Commissie overeenkomstig het ontwerpbesluit. In dit verband merkt het EDPB op dat wijzigingen in EO 14086 en het decreet van de Attorney General kunnen leiden tot de vaststelling van onmiddellijk toepasselijke uitvoeringshandelingen tot opschorting, intrekking of wijziging van het adequaatheidsbesluit²¹¹.

3.2.4.2 Voldoende onafhankelijkheid van de uitvoerende macht

222. In zijn arrest Schrems II heeft het Hof onderstreept dat de onafhankelijkheid van de rechterlijke instanties of de organen moet worden gewaarborgd, met name ten opzichte van de uitvoerende macht, met alle nodige waarborgen, ook wat betreft de voorwaarden voor ontslag of herroeping van de benoeming. Meer in het bijzonder heeft het Hof kritiek geuit op het feit dat de ombudsman is benoemd door en rechtstreeks rapporteert aan de minister van Buitenlandse Zaken. De ombudsman werd beschouwd als een integraal onderdeel van het Amerikaanse ministerie van Buitenlandse Zaken. Het Hof vond ook dat er geen bijzondere garanties waren voor het ontslag of de intrekking van de benoeming van de ombudsman, waardoor de onafhankelijkheid van de ombudsman ten opzichte van de uitvoerende macht werd ondermijnd.
223. Het EDPB erkent dat de bepalingen van EO 14086 en het aanvullende decreet van de Attorney General de DPRC niet verplichten verantwoording af te leggen aan de minister van Justitie, zoals het geval zou zijn in een relatie tussen een meerdere en een ondergeschikte. De DPRC valt evenmin onder het “dagelijks toezicht” van de minister van Justitie²¹². Deze waarborgen zijn een aanzienlijke verbetering ten opzichte van het privacyschild. De DPRC is echter opgericht binnen de uitvoerende macht, namelijk het ministerie van Justitie. Met name om deze reden zullen de uitvoering en de doeltreffende werking van de waarborgen in de praktijk van doorslaggevend belang zijn om te bepalen of de DPRC, hoewel deze geen integrerend deel uitmaakt van het ministerie van Justitie, als een niettemin binnen de uitvoerende macht gevestigde entiteit, in de praktijk als voldoende onafhankelijk kan worden beschouwd. Het EDPB verzoekt de Commissie zorgvuldig na te gaan of deze waarborgen volledig in de praktijk worden toegepast. Bovendien stelt het EDPB voor de term “dagelijks toezicht” zodanig te

²¹⁰ Zie Hof, C-487/19, arrest van 6 oktober 2021, W.Ž, ECLI:EU:C:2021:798 en C-132/20, arrest van 29 maart 2022, Getin Noble Bank S.A., ECLI:EU:C:2022:235, respectievelijk punt 129 en punt 121.

²¹¹ Ontwerpbesluit, overweging 212.

²¹² Decreet van de Attorney General, § 201.7, (d).

verduidelijken dat de “rechters” van de DPRC aan geen enkele vorm van toezicht zijn onderworpen. De Commissie heeft bevestigd dat “dagelijks toezicht” in deze zin moet worden opgevat.

224. Naast bovengenoemde waarborgen voorziet het EU-VS-DPF in bepaalde garanties met betrekking tot de benoeming en het ontslag van de “rechters” van de DPRC. Hoewel zij worden benoemd door de minister van Justitie, is hun benoeming gebaseerd op de criteria die worden gebruikt om kandidaten voor federale rechterlijke ambten te evalueren en wordt de PCLOB geraadpleegd. Ontslag van “rechters” vóór het verstrijken van hun ambtstermijn of van een lopende procedure is alleen mogelijk in strikt omschreven omstandigheden, die, zoals het EDPB begrijpt, zijn gebaseerd op de bepalingen die van toepassing zijn op federale rechters²¹³. De toepassing van deze regels vormt een verdere stap ter versterking van de onafhankelijke positie van de DPRC, waarvan ook hier de uitvoering in de praktijk cruciaal zal zijn. Uit het ontwerpbesluit als zodanig wordt echter niet duidelijk of en hoe de naleving van deze vereisten in de Verenigde Staten zal worden nagegaan. Op basis van aanvullende toelichtingen van de Commissie en de Amerikaanse regering begrijpt het EDPB dat de PCLOB de bovengenoemde bepalingen kan behandelen in zijn jaarlijkse evaluatie van het verhaalmechanisme en dat de verantwoordelijkheid van de inspecteur-generaal binnen het ministerie van Justitie voor het toezicht op en de naleving van alle wettelijke voorschriften, de vereisten in EO 14086 en de voorschriften (“regulations”) tot oprichting van de DPRC omvat. Het EDPB verzoekt de Commissie dit aspect in het ontwerpbesluit te verduidelijken. Dit gezegd zijnde, moet de Commissie met deze waarborgen rekening houden bij het toezicht op de feitelijke praktijk van de verwerking van persoonsgegevens zoals beoordeeld in het ontwerpbesluit.
225. Het ontwerpbesluit gaat niet in op de vraag of, en zo ja, onder welke voorwaarden de president van de VS de bevoegdheid heeft “rechters” van de DPRC te ontslaan of af te zetten. Het EDPB gaat ervan uit dat een dergelijke bevoegdheid niet bestaat, zoals de Europese Commissie heeft uitgelegd en door vertegenwoordigers van de Amerikaanse overheid is bevestigd. Het EDPB stelt voor dit aspect in het adequaatheidsbesluit te verduidelijken.
226. De “rechters” van de DPRC worden benoemd voor een hernieuwbare termijn van vier jaar en mogen op het moment van hun eerste benoeming de afgelopen twee jaar niet in de uitvoerende macht werkzaam zijn geweest²¹⁴. Tijdens hun aanstelling als “rechter” in de DPRC mogen zij geen andere officiële taken of functies binnen de Amerikaanse regering uitoefenen²¹⁵. Anders dan federale rechters in de VS kunnen zij echter wel deelnemen aan buitengerechtelijke activiteiten, waaronder zakelijke activiteiten, financiële activiteiten, fondsenwerving zonder winstoogmerk, fiduciaire activiteiten en de advocatuur, mits deze activiteiten de onpartijdige uitoefening van hun ambt of de doeltreffendheid of onafhankelijkheid van de DPRC niet in de weg staan²¹⁶. Rechterlijke onafhankelijkheid vloeit niet alleen voort uit de vrijheid van instructies, maar ook uit persoonlijke onafhankelijkheid. In dit verband zijn factoren als de ambtstermijn, de mogelijkheid tot herbenoeming en de mogelijkheid van belangenconflicten relevant. De termijn van vier jaar waarin EO 14086 respectievelijk het decreet van de Attorney General voorziet, is weliswaar korter dan de ambtstermijnen van de rechters van het Hof (zes jaar met de mogelijkheid van herbenoeming) en het EHRM (negen jaar zonder de mogelijkheid van herbenoeming), maar geeft als zodanig geen aanleiding tot ernstige bezorgdheid. Het EDPB is niet op de hoogte van enige jurisprudentie die in dit verband een minimale ambtstermijn oplegt²¹⁷. Het EDPB erkent tevens dat de mogelijkheid om buitengerechtelijke activiteiten te ontplooiën afhankelijk

²¹³ EO 14086, sectie 3, (d), (iv); decreet van de Attorney General § 201.7.

²¹⁴ Decreet van de Attorney General § 201.3, (a).

²¹⁵ Decreet van de Attorney General § 201.3, (c).

²¹⁶ Decreet van de Attorney General § 201.7, (c).

²¹⁷ Zie *mutatis mutandis* ook EHRM (Grote Kamer), zaak Centrum för rättsvisa/Zweden, 25 mei 2021, punt 346.

is van de voorwaarde dat deze, eenvoudig gezegd, niet mogen leiden tot belangenconflicten die de taken van de DPRC in het gedrang brengen. Het EDPB begrijpt uit de aanvullende toelichting van de Amerikaanse regering dat deze vereisten ook onderworpen zijn aan de toetsing en het toezicht door de PCLOB en de inspecteur-generaal van het ministerie van Justitie (zie punt 226). Hoe deze eis in de praktijk zal worden toegepast en aangetoond, moet eveneens in het kader van de gezamenlijke evaluaties worden behandeld.

227. Krachtens sectie 3, (d), (i), (B), EO 14086 moeten alle “rechters” van de DPRC in het bezit zijn van een veiligheidsmachtiging om toegang te kunnen krijgen tot gerubriceerde informatie, d.w.z. om hun eigenlijke functie, de berechting van zaken van nationale veiligheid, te kunnen uitvoeren²¹⁸. Sommige Europese wet- en regelgeving inzake veiligheidsmachtigingen stelt rechters daarentegen vrij van de eis van een veiligheidsmachtiging voor zover zij gerechtelijke taken vervullen, omdat een dergelijke gedetailleerde controle in strijd zou kunnen zijn met de onafhankelijkheid van de rechterlijke macht²¹⁹. Volgens verklaringen van de Amerikaanse regering wordt een kandidaat voor een rechterlijke benoeming in een Amerikaanse rechtbank weliswaar grondig doorgelicht, maar hoeft een federale rechter na zijn of haar benoeming tot rechter in een Amerikaanse rechtbank geen veiligheidsmachtiging te verkrijgen om toegang te krijgen tot gerubriceerde documenten die relevant zijn voor de zaak.
228. Naar de mening van het EDPB brengen de hierboven geschetste omstandigheden deels verschillen aan het licht tussen de positie en status van een Amerikaanse federale rechter en een “rechter” in de DPRC. De geboden waarborgen geven echter geen aanleiding om te twifelen aan de onafhankelijkheid van de DPRC. Het EDPB dringt er bij de Commissie op aan dat, indien het ontwerpbesluit wordt vastgesteld, de bovengenoemde waarborgen een prioriteit vormen tijdens de eerste gezamenlijke evaluatie van het EU-VS-DPF. Voorts verwacht het EDPB dat de Commissie haar toezegging nakomt om het besluit, indien vastgesteld, op te schorten, in te trekken of te wijzigen indien de Amerikaanse regering ervoor kiest de in het EO opgenomen waarborgen te beperken²²⁰.

3.2.4.3 Bevoegdheden van de DPRC

3.2.4.3.1 Toegang tot informatie

229. Een doeltreffende rechtsbescherming vereist dat een rechter over voldoende onderzoeksbevoegdheden beschikt om de bestreden maatregel te toetsen. In de zaak Kadi II oordeelde het Hof met betrekking tot artikel 47 van het Handvest dat de rechterlijke instanties van de Europese Unie ervoor moeten zorgen dat een beslissing op een voldoende solide feitelijke grondslag berust²²¹. Het Hof verklaart dat “[d]e Unierechter voor dat onderzoek in voorkomend geval de bevoegde autoriteit van de Unie [moet] verzoeken om overlegging van voor een dergelijk onderzoek relevante informatie en bewijzen, vertrouwelijk of niet”²²², waarbij “de geheimhouding of de vertrouwelijkheid van die informatie of dat bewijs niet kan worden tegengeworpen”²²³.
230. Overeenkomstig overweging 181 van het ontwerpbesluit toetst de DPRC de vaststellingen van de CLPO ten minste op basis van het verslag van het onderzoek van de CLPO, alsmede op basis van alle

²¹⁸ Zie ook decreet van de Attorney General § 201.11, (b) en ontwerpbesluit, overweging 177.

²¹⁹ Bv. § 2, (3), van de Duitse wet inzake veiligheidsmachtigingen.

²²⁰ Ontwerpbesluit, overweging 212.

²²¹ Hof, gevoegde zaken C-584/10 P, C-593/10 P en C-595/10 P, Europese Commissie e.a./Yassin Abdullah Kadi, arrest van 18 juli 2013 (hierna: arrest Kadi II van het Hof), punt 119.

²²² Arrest Kadi II van het Hof, punt 120.

²²³ Arrest Kadi II van het Hof, punt 125.

informatie en opmerkingen van de klager, de bijzondere jurist (*special advocate*) of een inlichtingendienst. In het ontwerpbesluit staat voorts dat de DPRC toegang heeft tot alle nodige informatie, die hij via de CLPO kan verkrijgen. Dit is gebaseerd op de bepaling van § 201.9(b) van het decreet van de Attorney General, op grond waarvan de DPRC kan verzoeken dat de CLPO van het ODNI het dossier aanvult met specifieke verklarende of verduidelijkende informatie en dat het de CLPO van het ODNI aanvullende feitelijke vaststellingen doet indien dat nodig is om het DPRC-panel in staat te stellen zijn evaluatie uit te voeren. Het EDPB gaat ervan uit dat de beoordeling door de DPRC dus geenszins beperkt blijft tot de bevindingen van de CLPO op het eerste niveau van het nieuwe verhaalmechanisme. Integendeel, de DPRC kan zowel aanvullende juridische informatie als, wat belangrijk is, verdere informatie over de feitelijke omstandigheden inwinnen voor zijn analyse van de vraag of een onder EO 14086 vallende schending heeft plaatsgevonden. Tegelijkertijd merkt het EDPB op dat deze over het algemeen uitgebreide onderzoeksbevoegdheden zich niet uitstrekken tot directe toegang tot de gegevens die over de persoon worden bijgehouden. De Commissie heeft uitgelegd dat de CLPO altijd als tussenpersoon zal fungeren wanneer de DPRC nadere informatie nodig heeft. De toegang van de DPRC tot de informatie die nodig is om zich onafhankelijk over een verzoek om toetsing uit te spreken, hangt derhalve tot op zekere hoogte af van de vraag of de CLPO de nodige informatie verstrekt. Het EDPB erkent dat de CLPO verplicht is de DPRC “alle nodige steun” te verlenen en dat de inlichtingendiensten verplicht zijn de CLPO toegang te verlenen tot de informatie die nodig is voor de toetsing door de DPRC²²⁴. Het EDPB merkt echter ook op dat de CLPO zelf niet onafhankelijk is en in de eerste fase van de verhaalprocedure het eerste onderzoek van een klacht verricht. Daarom juicht het EDPB toe dat de PCLOB tijdens zijn jaarlijkse evaluaties van het verhaalmechanisme zal nagaan of de DPRC volledige toegang heeft gekregen tot alle noodzakelijke informatie²²⁵. Bovendien verzoekt het EDPB de Commissie dit aspect op te nemen in de gezamenlijke evaluaties, indien het ontwerpbesluit wordt vastgesteld, om de gevolgen van dit systeem in de praktijk te onderzoeken.

3.2.4.3.2 *Corrigerende bevoegdheden*

231. Een van de centrale tekortkomingen van het privacyschild die tot de ongeldigverklaring ervan door het Hof in Schrems II hebben geleid, was het ontbreken van bindende corrigerende bevoegdheden voor de ombudsman. Het Hof oordeelde dat “nergens uit dit besluit [blijkt] dat deze ombudsman bevoegd is om bindende beslissingen te nemen ten aanzien van deze [inlichtingen]diensten”²²⁶. De loutere (politieke) toezegging van de Amerikaanse regering dat de inlichtingendiensten elke door de ombudsman geconstateerde schending van de toepasselijke regels zou corrigeren, volstond niet om een beschermingsniveau te waarborgen dat in wezen gelijk is aan het niveau dat in artikel 47 van het Handvest wordt gewaarborgd.
232. In het nieuwe verhaalmechanisme daarentegen hebben de besluiten van de CLPO en de DPRC bindende werking²²⁷. Het EDPB erkent enerzijds dat deze bevoegdheid niet beperkt is tot specifieke maatregelen, maar “passende herstelmaatregelen” toestaat om een vastgestelde onder EO 14086 vallende schending “volledig te herstellen”. Met name sectie 4, (a), EO 14086 vermeldt uitdrukkelijk de schrapping van onrechtmatig verzamelde gegevens. Anderzijds merkt het EDPB op dat de formulering van sectie 4, (a), EO 14086 enige onzekerheid schept over het proces om dergelijk “passend herstel” te bepalen. Hoewel een maatregel bedoeld moet zijn om een schending volledig ongedaan te maken, moet ook rekening worden gehouden met de manieren waarop een dergelijke

²²⁴ EO 14086, sectie 3, (c), (i), (H) en sectie 3, (d), (iii).

²²⁵ EO 14086, sectie 3, (e), (i).

²²⁶ Arrest Schrems II van het Hof, punt 196.

²²⁷ EO 14086, respectievelijk sectie 3, (c), (ii), en sectie 3, (d), (ii).

schending gewoonlijk wordt aangepakt²²⁸. De betekenis en de uitwerking van dit vereiste zijn onduidelijk. Daarom verzoekt het EDPB de Commissie de in de praktijk genomen herstelmaatregelen nauwlettend te monitoren.

3.2.4.4 Een klacht indienen in het kader van het nieuwe verhaalmechanisme

233. Het bij EO 14086 ingestelde verhaalmechanisme is alleen van toepassing op in aanmerking komende klachten die door de bevoegde overheidsinstantie in een in aanmerking komende staat worden ingediend over SIGINT-activiteiten van de Verenigde Staten voor een onder EO 14086 vallende schending²²⁹. Om van deze rechtsbescherming gebruik te kunnen maken, moet dus aan een aantal voorwaarden worden voldaan.

3.2.4.4.1 Aanwijzing als in aanmerking komende staat

234. In de eerste plaats moet het land of de regionale organisatie voor economische integratie, van waaruit de gegevens naar de Verenigde Staten zijn doorgegeven, vóór de gegevensoverdracht die aan de klacht ten grondslag ligt, zijn aangewezen als in aanmerking komende staat²³⁰. Het is uiteraard van essentieel belang dat het geboden verhaalmechanisme beschikbaar is wanneer het adequaatheidsbesluit van toepassing wordt. Overweging 196 van het ontwerpbesluit bepaalt dan ook dat de inwerkingtreding van het besluit onder meer afhankelijk is van de aanwijzing van de Unie als in aanmerking komende entiteit voor de toepassing van het verhaalmechanisme. In feite lijkt de Commissie ervan uit te gaan dat de aanwijzing zal plaatsvinden vóór de vaststelling van het besluit, aangezien het ontwerp reeds een plaatshouder bevat voor de aanwijzing van de EU²³¹ door de minister van Justitie (in tegenstelling tot het opnemen van de aanwijzing als opschortende voorwaarde in het dispositief van het ontwerpbesluit).

3.2.4.4.2 Nadelige gevolgen voor de privacy en de burgerlijke vrijheden en belang bij het aanhangig maken van een procedure

235. Een “in aanmerking komende klacht” moet gebaseerd zijn op een vermeende “onder EO 14086 vallende schending”, wat op zijn beurt een schending vereist die de individuele privacy en burgerlijke vrijheden van de klager aantast²³². Het EDPB gaat er, op basis van aanvullende uitleg van de Commissie, van uit dat “nadelige gevolgen” geen enkele vorm van beperking van de ontvankelijkheid van een klacht inhoudt. Zoals de Commissie verklaarde, zouden dergelijke nadelige gevolgen veeleer betrekking hebben op elke klacht betreffende de verwerking van persoonsgegevens voor SIGINT-activiteiten in strijd met de in sectie 4, (d), (iii), bedoelde bepalingen, bijvoorbeeld de waarborgen van EO 14086. Het EDPB betreurt dat dit niet in de tekst van het ontwerpbesluit wordt gespecificeerd en verzoekt de Commissie het begrip “nadelige gevolgen” nader te verduidelijken om ervoor te zorgen dat elke schending van de rechten van de betrokkenen wordt beoordeeld en verholpen en dat er geen niveau van “ernst” hoeft te worden aangetoond om toegang te krijgen tot rechtsmiddelen en passende herstelmaatregelen.
236. Zoals reeds vermeld, hoeft de eiser voor een klacht uit hoofde van EO 14086 geen belang bij het aanhangig maken van een procedure aan te tonen (zie punt 215)²³³. Het EDPB verwelkomt de

²²⁸ EO 14086, sectie 4, (a).

²²⁹ EO 14086, sectie 3, (a).

²³⁰ EO 14086, sectie 4, (d), (i) en sectie 4, (k), (i).

²³¹ Ontwerpbesluit, voetnoot 320.

²³² EO 14086, sectie 4, (k), (i) en sectie 4, (d), (ii).

²³³ Clapper/Amnesty International USA, 568 U.S. 398 (2013) II., blz. 10.

verduidelijking in sectie 4, (k), EO 14086 dat een “overtuigingstoets” (*belief test*) zal worden toegepast en dat niet hoeft te worden aangetoond dat er via SIGINT-activiteiten feitelijk toegang is geweest tot de gegevens van de klager. De instelling van het verhaalmechanisme is een belangrijke stap, aangezien het vereiste van belang bij het aanhangig maken van een procedure het erg moeilijk maakt om surveillancemaatregelen aan te vechten voor gewone rechters in de Verenigde Staten.

237. Op basis van het bovenstaande is het EDPB van mening dat een beroep op de gewone rechter, waarnaar in het ontwerpbesluit ook wordt verwezen²³⁴, geen adequaat beschermingsniveau biedt²³⁵. In dit verband herinnert het EDPB aan zijn reeds vele malen geuite bezorgdheid met betrekking tot het vereiste van belang bij het aanhangig maken van een procedure voor de gewone rechter²³⁶. Bovendien meent het EDPB, op basis van aanvullende verklaringen van de Amerikaanse regering, dat EO 14086 weliswaar een beroep op de gewone rechter niet uitsluit, maar dat het onzeker is hoe een dergelijke rechter dit EO zou toepassen. Deze kwestie kan verder worden onderzocht bij de toekomstige evaluaties, indien het ontwerpbesluit wordt vastgesteld.

3.2.4.4.3 *De procedure van een klacht*

238. Het EDPB onderschrijft in beginsel de procedure voor het leiden van een klacht via de toezichthoudende autoriteiten van de lidstaten en blijft van mening dat de identificatie van de klager op het grondgebied van de EU moet plaatsvinden. Evenals bij het mechanisme van de privacyschildombudsman bepaalt het ontwerpbesluit echter dat een betrokkene die een dergelijke klacht wil indienen, deze moet indienen bij een toezichthoudende autoriteit in een EU-lidstaat die bevoegd is voor het toezicht op de nationale veiligheidsdiensten en/of de verwerking van persoonsgegevens door overheidsdiensten²³⁷. In dit verband herinnert het EDPB aan zijn reeds in het advies van de Groep gegevensbescherming artikel 29 over het privacyschild geuite bezorgdheid, bijvoorbeeld over mogelijke problemen voor personen om de bevoegde autoriteit te identificeren, gezien de verscheidenheid aan toezichtmechanismen op nationale veiligheidsdiensten in de lidstaten²³⁸. Gelet op de betrokkenheid van de nationale gegevensbeschermingsautoriteiten bij de toepassing van en het toezicht op het EU-VS-DPF is het passender de klachten via hen te laten verlopen.

3.2.4.5 *Het besluit van de DPRC*

239. Nadat het onderzoek van de aanvraag van de klager is afgerond, mag de DPRC niet bekendmaken of de klager al dan niet onderworpen was aan Amerikaanse SIGINT-activiteiten. In plaats daarvan wordt de klager meegedeeld dat het onderzoek geen onder EO 14086 vallende schendingen aan het licht heeft gebracht of dat de Data Protection Review Court een besluit heeft genomen dat passende herstelmaatregelen vereist²³⁹. Dit standaardantwoord dient het algemeen legitieme doel om gevoelige informatie over Amerikaanse inlichtingenactiviteiten te beschermen. Het EDPB vreest echter dat EO 14086 niet voorziet in uitzonderingen op het standaardantwoord van de DPRC.
240. In de zaak Kadi II moest het Hof zich buigen over de tegenstrijdige belangen van staatsgeheim enerzijds en een eerlijke procedure, voor zover mogelijk met hoor en wederhoor anderzijds. Het Hof oordeelde dat in gevallen waarin dwingende overwegingen in verband met nationale veiligheid zich ertegen

²³⁴ Ontwerpbesluit, overweging 187 en volgende.

²³⁵ Arrest Schrems II van het Hof, punten 191-192.

²³⁶ Advies 01/2016 van de Groep gegevensbescherming artikel 29, blz. 43.

²³⁷ Ontwerpbesluit, overweging 169.

²³⁸ Advies 01/2016 van de Groep gegevensbescherming artikel 29, blz. 48-49.

²³⁹ EO 14086, sectie 3, (d), (i), (H). Sectie van EO 14086 bepaalt dit antwoord ook voor de CLPO.

verzetten dat bepaalde informatie of bepaald bewijs aan de betrokken persoon wordt meegedeeld, het evenwel aan de rechter staat om bij de uitoefening van zijn rechterlijke toetsing zodanige technieken te hanteren dat gerechtvaardigde overwegingen van zekerheid omtrent de aard en de bronnen van de inlichtingen die bij de vaststelling van de betrokken handeling in aanmerking zijn genomen, kunnen worden verzoend met de noodzaak om de justitiabele voldoende procedurele bescherming te bieden, zoals het recht om te worden gehoord en het beginsel van hoor en wederhoor²⁴⁰. Het Hof heeft voorts gepreciseerd dat de Unierechter door een onderzoek van alle door de bevoegde autoriteit van de Unie verstrekte gegevens feitelijk en rechtens moet nagaan of de door die autoriteit aangevoerde redenen om zich te verzetten tegen een dergelijke mededeling gegrond zijn²⁴¹. Blijkt dat de door de bevoegde autoriteit van de Europese Unie aangevoerde redenen zich daadwerkelijk verzetten tegen de mededeling van informatie en bewijzen aan de betrokken persoon, dan moet op passende wijze een evenwicht worden gezocht tussen de vereisten die samenhangen met het recht op effectieve rechterlijke bescherming en de vereisten die voortvloeien uit de nationale veiligheid²⁴². Voor een dergelijke afweging kan worden teruggegrepen naar mogelijkheden zoals de mededeling van een samenvatting van de inhoud van de betreffende informatie en bewijzen²⁴³. Hoewel de bevindingen van het Hof geen eisen stellen aan de beslissing van een rechter, maar betrekking hebben op de beslissing van de bevoegde autoriteit en het verloop van de gerechtelijke procedure, geven zij aanwijzingen over de afweging van de bovengenoemde belangen in het kader van het recht op effectieve rechtsbescherming. Voor verdere aanwijzingen kan ook worden verwezen naar de zaak Big Brother Watch, waarin het EHRM, onder verwijzing naar de eerlijkheid van de procedure en met name naar het beginsel van hoor en wederhoor, heeft geoordeeld dat de beslissingen van een rechterlijke of anderszins onafhankelijke instantie met redenen moeten worden omkleed²⁴⁴.

241. Het EDPB erkent dat de besluiten van de DPRC wel degelijk gemotiveerd zijn. Er wordt uitdrukkelijk vereist dat de DPRC een schriftelijk besluit neemt waarin zijn bevindingen en de specificatie van een passende herstelmaatregel zijn opgenomen²⁴⁵. Bovendien merkt het EDPB op dat de betrokkene zal worden ingelicht indien de informatie betreffende een toetsing door de DPRC is gederubriceerd²⁴⁶. Het EDPB erkent ook de rol van de in het nieuwe verhaalmechanisme voorziene bijzondere juristen (*special advocates*), die onder meer de belangen van de klager in de zaak behartigen²⁴⁷. In het licht van de implicaties van de hierboven uiteengezette jurisprudentie van het Hof en het EHRM en rekening houdend met het feit dat tegen het besluit van de DPRC geen beroep kan worden ingesteld maar dat het definitief is²⁴⁸, heeft het EDPB evenwel bedenkingen bij de algemene toepassing van het standaardantwoord van de DPRC. Het EDPB herinnert eraan dat de PCLOB de werking van het nieuwe verhaalmechanisme onafhankelijk zal evalueren en verzoekt de Commissie bij toekomstige evaluaties van het besluit, indien dit wordt vastgesteld, bijzondere aandacht aan dit punt te besteden, met inbegrip van een beoordeling van dit aspect door de PCLOB.

²⁴⁰ Arrest Kadi II van het Hof, punt 125.

²⁴¹ Arrest Kadi II van het Hof, punt 126.

²⁴² Arrest Kadi II van het Hof, punt 128.

²⁴³ Arrest Kadi II van het Hof, punt 129.

²⁴⁴ Zie EHRM-arrest Big Brother Watch, punt 359.

²⁴⁵ Decreet van de Attorney General, § 201.9, (g).

²⁴⁶ EO 14086, sectie 3, (d), (v).

²⁴⁷ Decreet van de Attorney General, § 201.8, (g).

²⁴⁸ Decreet van de Attorney General, § 201.9, (g).

4 UITVOERING VAN EN MONITORING OP HET ONTWERPBESLUIT

242. Met betrekking tot de monitoring op en de evaluatie van het ontwerpbesluit merkt het EDPB op dat volgens de rechtspraak van het Hof “het aan de Commissie [staat], met het oog op het feit dat het door een derde land geboden beschermingsniveau aan ontwikkelingen onderhevig kan zijn, om na de vaststelling van een beschikking krachtens [artikel 45 AVG] periodiek na te gaan of de constatering dat het door het derde land in kwestie geboden beschermingsniveau passend is, nog steeds in feite en in rechte gerechtvaardigd is. Een dergelijk onderzoek dringt zich in elk geval op wanneer er aanwijzingen zijn die daarover twijfels doen ontstaan”²⁴⁹.
243. Bovendien merkt het EDPB op dat de brief van het Amerikaanse ministerie van Handel bepaalt dat het ministerie van Handel en andere Amerikaanse diensten, naargelang het geval, op gezette tijden bijeenkomsten zullen houden met de Commissie, belanghebbende gegevensbeschermingsautoriteiten van de EU en passende vertegenwoordigers van het EDPB²⁵⁰.
244. Het EDPB is van mening dat de bescherming uit hoofde van de wetgeving van de staten met betrekking tot toegang door rechtshandavingsinstanties, de afwijking voor tijdelijke bulksgewijze verzameling met het oog op gerichte verzameling door Amerikaanse nationale veiligheidsdiensten, de toepassing in de praktijk van de onlangs ingevoerde beginselen van noodzakelijkheid en evenredigheid, ook in de context van het Upstream-programma, de wisselwerking tussen EO 14086 en de verschillende Amerikaanse rechtsinstrumenten die Amerikaanse inlichtingendiensten toestaan persoonsgegevens te verzamelen en verder te verwerken, de uitvoerende interne beleidsmaatregelen en procedures, de wijze waarop deze waarborgen ook in aanmerking zullen worden genomen in het kader van het door de FISC geleide toezicht, en de wijze waarop het verhaalmechanisme zal functioneren, en de kwestie van de verdere doorgifte, geautomatiseerde besluiten, inhoudelijk en doeltreffend toezicht op en handhaving van de DPF-beginselen, en doeltreffende verhaalsmogelijkheden, in de loop van de volgende periodieke evaluaties specifieke aandacht verdienen.
245. Het EDPB merkt op dat de evaluatie van de bevinding van adequaatheid één jaar na de datum van kennisgeving van het adequaatheidsbesluit aan de lidstaten en vervolgens ten minste om de vier jaar zal plaatsvinden²⁵¹. Om het permanente toezicht op het adequaatheidsbesluit verder te versterken, verzoekt het EDPB de Commissie de latere evaluaties ten minste om de drie jaar uit te voeren.
246. Wat betreft de praktische betrokkenheid van het EDPB en zijn vertegenwoordigers bij de voorbereiding en het verloop van de toekomstige periodieke evaluaties, herhaalt het EDPB dat alle relevante documentatie voldoende lang vóór de evaluaties schriftelijk met het EDPB moet worden gedeeld, met inbegrip van correspondentie. Evenals bij de evaluaties in het kader van het privacyschild beveelt het EDPB aan dat uiterlijk drie maanden voordat de evaluatie moet plaatsvinden, de modaliteiten voor de evaluatie worden vastgesteld en overeengekomen tussen de Commissie, de Amerikaanse regering en het EDPB.
247. Voorts merkt het EDPB op en verwelkomt hij dat overweging 212 van het ontwerpbesluit voorbeelden geeft van wijzigingen die het beschermingsniveau ondermijnen en die het inleiden van een “noodintrekkingsprocedure” kunnen rechtvaardigen, die gericht is op wijzigingen die zich zouden

²⁴⁹ Arrest Schrems I van het Hof, punt 76. Zie ook ontwerpbesluit, artikel 3, lid 4.

²⁵⁰ Ontwerpbesluit, bijlage III.

²⁵¹ Ontwerpbesluit, artikel 3, lid 4.

kunnen voordoen met betrekking tot Executive Order 14086 en het daarmee samenhangende decreet van de Attorney General.

Voor het Europees Comité voor gegevensbescherming

De voorzitter

(Andrea Jelinek)