WERKGROEP GEGEVENSBESCHERMING ARTIKEL29

16/NL
WP 238

Advies 01/2016 inzake het ontwerp-adequaatheidsbesluit betreffende het EU-VS privacyschild

Goedgekeurd op 13 april 2016

SAMENVATTING

Op 29 februari 2016 heeft de Europese Commissie een mededeling, een ontwerp-adequaatheidsbesluit en bijlagen gepubliceerd die samen een nieuw kader vormen voor de trans-Atlantische uitwisseling van persoonsgegevens voor commerciële doeleinden: het EU-VS privacyschild (hierna "het privacyschild" genoemd). Dit instrument heeft tot doel heeft de eerdere Amerikaanse veiligehavenbeschikking te vervangen, die op 6 oktober 2015 door het Hof van Justitie van de Europese Unie (HvJEU) in de zaak-Schrems ongeldig is verklaard.

In overeenstemming met artikel 30, lid 1, onder c), van Richtlijn 95/46/EG heeft de Groep artikel 29 (hierna WP29 genoemd) deze documenten beoordeeld om zich te kunnen uitspreken over het ontwerp-adequaatheidsbesluit. WP29 heeft zowel de commerciële aspecten beoordeeld als de mogelijkheden om van de beginselen van het privacyschild af te wijken omwille van de nationale veiligheid, rechtshandhaving en doeleinden van algemeen belang.

WP29 heeft daarbij rekening gehouden met het toepasselijke rechtskader inzake EU-gegevensbescherming zoals uiteengezet in Richtlijn 95/46/EG, alsmede met de grondrechten op eerbiediging van het privéleven en bescherming van persoonsgegevens, zoals opgenomen in artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie. Bovendien heeft WP29 het recht op een doeltreffende voorziening in rechte en op een eerlijk proces in aanmerking genomen, zoals vastgelegd in artikel 47 van het Handvest, alsmede de jurisprudentie met betrekking tot de diverse grondrechten.

Daarnaast weerspiegelt de analyse de redenering van het HvJEU in de zaak-Schrems inzake de beoordelingsmarge van de Commissie met betrekking tot een adequaatheidsbeoordeling. Het onderzoek en de controles van de adequaatheidsvereisten moeten strikt worden uitgevoerd, rekening houdend met de grondrechten op privacy en gegevensbescherming en met het aantal natuurlijke personen dat mogelijk gevolgen ondervindt van de doorgifte.

Het privacyschild moet worden bezien tegen de huidige internationale achtergrond, met inbegrip van de opkomst van big data en de toenemende behoefte aan beveiliging. De reikwijdte en de omvang van de verzameling en het gebruik van persoonsgegevens zijn fors toegenomen sinds de oorspronkelijke veiligehavenbeschikking in 2000 werd vastgesteld. Tegelijkertijd hameren Europese gegevensbeschermingsinstanties op het belang van de beginselen die zij verdedigen.

WP29 is op de eerste plaats ingenomen met de aanzienlijke verbeteringen die het privacyschild ten opzichte van de veiligehavenbeschikking met zich meebrengt. WP29 merkt op dat veel van de tekortkomingen van de veilige haven die de Groep bij brief van 10 april 2014 aan vicevoorzitter Reding heeft benadrukt, door de onderhandelaars zijn verholpen.

Doordat beginselen en garanties waarin het privacyschild voorziet in zowel het adequaatheidsbesluit als de bijlagen uiteengezet zijn, is de informatie moeilijk te vinden en

soms onsamenhangend. Dit vergroot de algehele onduidelijkheid met betrekking tot het nieuwe kader en beperkt de toegankelijkheid voor betrokkenen, organisaties en gegevensbeschermingsinstanties. Ook de gebezigde taal is onduidelijk. Daarom verzoekt WP29 de Commissie dringend om er voor te zorgen dat het kader duidelijk en begrijpelijk is voor beide zijden van de Atlantische Oceaan.

Met betrekking tot de toepasselijke wetgeving benadrukt WP29 dat, als het adequaatheidsbesluit over het privacyschild wordt goedgekeurd op basis van Richtlijn 95/46/EG, dit consistent moet zijn met het rechtskader inzake gegevensbescherming van de EU, zowel wat het toepassingsgebied als de terminologie betreft. WP29 is van mening dat kort na de inwerkingtreding van de algemene verordening gegevensbescherming een beoordeling moet worden uitgevoerd om ervoor te zorgen dat het hogere niveau van gegevensbescherming waarin de verordening voorziet, in het adequaatheidsbesluit en de bijlagen ervan wordt overgenomen.

Over de commerciële aspecten van het privacyschild

De belangrijkste doelstelling van WP29 is ervoor te zorgen dat bij de verwerking van persoonsgegevens volgens de bepalingen van het privacyschild er voor natuurlijke personen een in grote lijnen overeenkomstig niveau van bescherming wordt gehandhaafd. WP29 verwacht niet dat het privacyschild eenvoudigweg een volledige kopie wordt van het EU-rechtskader; wel is zij van mening dat het de kern moet bevatten van de fundamentele beginselen en dientengevolge een in grote lijnen overeenkomstig niveau van bescherming moet waarborgen.

Ondanks de door het privacyschild geboden verbeteringen, is WP29 van mening dat een aantal belangrijke, in het Europese recht vervatte gegevensbeschermingsbeginselen niet tot uitdrukking komt in het ontwerp-adequaatheidsbesluit en de bijlagen, of door onjuiste alternatieve begrippen is vervangen.

Het beginsel van gegevensbewaring wordt bijvoorbeeld niet expliciet genoemd en kan niet duidelijk worden afgeleid uit de huidige formulering van het beginsel van gegevensintegriteit en doelbinding. Voorts is er geen formulering over de bescherming die geboden zou moeten worden tegen geautomatiseerde individuele besluiten die uitsluitend op een geautomatiseerde gegevensverwerking berusten. De toepassing van het beginsel van doelbinding op gegevensverwerking is ook niet duidelijk. Teneinde meer duidelijkheid te scheppen over het gebruik van verschillende belangrijke begrippen, stelt WP29 voor dat de EU en de VS duidelijke definities afspreken die in een verklarende termenlijst in de FAQ van het privacyschild worden opgenomen.

Omdat het privacyschild ook zal worden gebruikt voor het overdragen van gegevens buiten de VS, stelt WP29 met klem dat verdere doorgifte vanuit een entiteit die onder het privacyschild valt, naar ontvangers in een derde land, gepaard moet gaan met dezelfde mate van bescherming met betrekking tot alle aspecten van het schild (met inbegrip van de nationale veiligheid) en niet moet leiden tot versoepeling of omzeiling van EU-

gegevensbeschermingsbeginselen. Als er een verdere doorgifte naar een derde land in het kader van het privacyschild wordt gepland, zou elke privacyschildorganisatie verplicht, en voorafgaand aan de doorgifte, alle bindende voorschriften van de op de gegevensimporteur van toepassing zijnde nationale wetgeving van het derde land moeten beoordelen. Over het algemeen concludeert WP29 dat verdere doorgifte van EU-persoonsgegevens onvoldoende geregeld is, vooral met betrekking tot het toepassingsgebied, de doelbinding en de garanties die van toepassing zijn op doorgiften aan vertegenwoordigers.

Ten slotte neemt WP29 nota van de aanvullende middelen die beschikbaar worden gesteld om natuurlijke personen hun rechten te laten uit uitoefenen, maar vreest zij dat het nieuwe verhaalsmechanisme in de praktijk te complex, moeilijk te gebruiken voor natuurlijke personen uit de EU en daardoor niet doeltreffend zal blijken te zijn. Nadere toelichting bij de diverse verhaalsprocedures is daarom nodig; in het bijzonder kunnen EU-gegevensbeschermingsautoriteiten, indien ze dat willen, tijdens de verschillende procedures als een natuurlijk contactpunt voor natuurlijke personen uit de EU worden beschouwd, omdat zij namens hen kunnen optreden.

Afwijkingen met het oog op de nationale veiligheid

Met betrekking tot de toegang tot gegevens door overheidsdiensten, zowel in de EU als in derde landen, herinnert WP29 aan haar analyse van de betrokken grondrechten, die is opgenomen in het werkdocument over de rechtvaardiging van de inperking van de grondrechten op privacy en gegevensbescherming door middel van toezichtsmaatregelen bij de doorgifte van persoonsgegevens (Europese essentiële waarborgen) (WP237).

Een grote stap voorwaarts ten opzichte van de veiligehavenbeschikking is dat het ontwerp-adequaatheidsbesluit nu uitgebreid ingaat op de mogelijke toegang tot conform het privacyschild verwerkte gegevens met het oog op de nationale veiligheid en rechtshandhaving. WP29 neemt nota van deze belangrijke stap en van de toegenomen transparantie van de Amerikaanse regering over de wetgeving die van toepassing is op het verzamelen van inlichtingen (bijlage VI).

WP29 merkt echter op dat de vertegenwoordigingen van het Amerikaanse bureau van de directeur van de nationale inlichtingendienst (U.S. Office of the Director of National Intelligence, ODNI), de grootschalige en willekeurige verzameling van persoonsgegevens uit de EU niet uitsluiten. WP29 wijst eens te meer op haar standpunt dat grootschalig en willekeurig toezicht op natuurlijke personen in een democratische maatschappij nooit kan worden beschouwd als evenredig en strikt noodzakelijk, zoals vereist is voor de door de toepasselijke grondrechten geboden bescherming. Bovendien is breed toezicht op alle toezichtsprogramma's van cruciaal belang. WP29 neemt nota van de bestaande tendens om in het licht van de strijd tegen terrorisme steeds meer gegevens op grootschalige en willekeurige wijze te verzamelen. Gezien de zorgen die deze ontwikkeling met zich meebrengt voor de bescherming van de grondrechten op privacy en gegevensbescherming, ziet WP29 uit naar de arresten van het HvJEU in zaken met betrekking tot grootschalige en willekeurige gegevensverzameling.

Wat het recht op verhaal betreft, juicht WP29 de aanstelling van een ombudsman als een nieuw verhaalsmechanisme toe. Dit kan een aanzienlijke verbetering betekenen voor de rechten van natuurlijke personen uit de EU met betrekking tot activiteiten van Amerikaanse inlichtingendiensten. WP29 is echter bezorgd dat dit nieuwe instituut onvoldoende onafhankelijk is, niet over de juiste bevoegdheden beschikt om zijn taak doeltreffend te vervullen en geen bevredigende oplossing in geval van betwisting garandeert.

Gezamenlijke evaluatie

Het mechanisme van jaarlijkse gezamenlijke evaluatie, zoals genoemd in het ontwerp-adequaatheidsbesluit, is van groot belang voor de algemene geloofwaardigheid van het privacyschild en WP29 is zeer ingenomen met de gelegenheid die middel zou bieden om het adequaatheidsbesluit te evalueren. WP29 begrijpt dat nationale vertegenwoordigers van WP29 volledig kunnen deelnemen aan het evaluatieproces, maar vraagt om een toelichting met betrekking tot de specifieke regelingen. De bijzonderheden (met inbegrip van betrokken verslag, de bijbehorende publiciteit en de mogelijke gevolgen daarvan, alsmede de financiering) moeten ruim vóór de eerste evaluatie worden overeengekomen.

Conclusie

WP29 neemt nota van de belangrijke verbeteringen die het privacyschild biedt ten opzichte van de ongeldig verklaarde veiligehavenbeschikking. Gezien voornoemde punten van zorg en het verzoek om toelichting, dringt WP29 er bij de Commissie op aan om deze zorgen weg te nemen, met passende oplossingen te komen en de gevraagde toelichting te verschaffen teneinde het ontwerp-adequaatheidsbesluit te verbeteren en ervoor te zorgen dat de door het privacyschild geboden bescherming daadwerkelijk in grote lijnen overeenkomt met die van de EU.

INHOUDSOPGAVE

1. INLEIDING

Naar aanleiding van het arrest van het Hof van Justitie van de Europese Unie (HvJEU) van 6 oktober 2015 in de zaak-Schrems[1], heeft de Groep artikel 29 (hierna "WP29" of "de werkgroep" genoemd) de lidstaten van de Europese Unie en de Europese instellingen verzocht om in gesprek te gaan met de autoriteiten van de Verenigde Staten teneinde politieke, juridische en technische oplossingen te zoeken om het mogelijk te maken gegevens door te geven naar het Amerikaanse grondgebied met inachtneming van de grondrechten.

Op 2 februari 2016 bereikten de Europese Commissie en het Amerikaanse Ministerie van Handel (DoC), na meer dan twee jaar onderhandelen, een politiek akkoord over een nieuw kader voor de trans-Atlantische uitwisselingen van persoonsgegevens voor handelsdoeleinden: het EU-VS privacyschild (hierna "het privacyschild" genoemd). Dit instrument moet de eerdere Amerikaanse veiligehavenbeschikking vervangen.

Op 29 februari 2016 publiceerde de Commissie een mededeling[2], een ontwerp-adequaatheidsbesluit en de bijlagen die het privacyschild zullen vormen. In overeenstemming met artikel 30, lid 1, onder c), van Richtlijn 95/46/EG (hierna "de richtlijn" genoemd) heeft WP29 deze documenten beoordeeld teneinde haar advies te geven over het door de Commissie voorbereide ontwerp-adequaatheidsbesluit, inclusief de onderliggende documenten over het privacyschild. Daarbij heeft WP29 enerzijds het commerciële deel van het privacyschild beoordeeld en anderzijds een analyse gemaakt van de waarborgen in verband met mogelijkheden om van de beginselen van het privacyschild af te wijken omwille van de nationale veiligheid, wetshandhaving en doeleinden van algemeen belang.

Naar aanleiding van het arrest in de zaak-Schrems, heeft WP29 een aantal bijeenkomsten belegd met afgevaardigden van de Amerikaanse regering, vertegenwoordigers van maatschappelijke organisaties uit de EU en de VS, en wetenschappers, om de beoordeling van de gevolgen van het arrest-Schrems voor te bereiden. Tijdens de beoordeling van het privacyschild zijn verdere bijeenkomsten met de Europese Commissie en vertegenwoordigers van de Amerikaanse regering gehouden. Tijdens deze bijeenkomsten werd enige toelichting verstrekt waarmee in dit advies eveneens rekening is gehouden. WP29 benadrukt dat deze toelichting vooralsnog louter informeel is en niet als integrerend onderdeel van het ontwerp-adequaatheidsbesluit kan worden beschouwd, daar de uitleg nog niet schriftelijk is vastgelegd.

Niettemin verwelkomt WP29 in het bijzonder de toezegging die het DoC op deze bijeenkomsten heeft gedaan, nl. om samen te werken met de gegevensbeschermingsautoriteiten in de EU-lidstaten op het gebied van de toepassing van het privacyschild en om op hun websites instructies en juridische uitleg te verschaffen over de toepassing van het privacyschild.

[1] Zaak C-362/14, Maximilian Schrems tegen Data Protection Commissioner, 6 oktober 2015 (hierna "de zaak-Schrems" genoemd).
[2] COM(2016) 117 definitief, 29 februari 2016,

1.1 Algemene opmerkingen

1.1.1. Reikwijdte van de beoordeling van WP29

WP29 heeft het toepasselijke gegevensbeschermingskader in de lidstaten van de Europese Unie in aanmerking genomen, met inbegrip van artikel 8 van het Europees Verdrag voor de rechten van de mens (EVRM), dat strekt tot bescherming van het recht op eerbiediging van het privéleven en het familie- en gezinsleven, alsmede de artikelen 7, 8 en 47 van het Handvest van de grondrechten van de Europese Unie, waarin het recht op privé- en gezinsleven, het recht op bescherming van persoonsgegevens en het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht worden beschermd. Bovendien heeft WP29 de relevante jurisprudentie, alsmede de vereisten van de richtlijn in aanmerking genomen.

De vereiste dat een derde land een passend niveau van gegevensbescherming moet waarborgen, is door het HvJEU in de zaak-Schrems nader uitgewerkt. Het Hof heeft niet alleen uitgelegd dat de bepalingen van de richtlijn moeten worden uitgelegd "op basis van de grondrechten die door het Handvest worden gewaarborgd"[3] en dan met name in de artikelen 7 en 8 daarvan, maar ook duidelijk gemaakt dat de uitdrukking "passend beschermingsniveau" zo moet worden opgevat dat die "vereist dat het derde land, op grond van zijn nationale wetgeving of zijn internationale verbintenissen, een niveau van bescherming van de grondrechten en de fundamentele vrijheden biedt dat in grote lijnen overeenkomt met het niveau dat binnen de Unie wordt gewaarborgd op grond van Richtlijn 95/46, gelezen in samenhang met het Handvest"[4]. Met betrekking tot de eerdere veiligehavenbeschikking is een dergelijke beoordeling nooit voldoende gedetailleerd verricht. WP29 heeft het ontwerp-adequaatheidsbesluit daarom geanalyseerd in het licht van de vereiste te beoordelen of het niveau van bescherming van grondrechten en fundamentele vrijheden *in grote lijnen overeenkomt* met het binnen de EU gewaarborgde beschermingsniveau. WP29 benadrukt dat dit advies haar belangrijkste punten van zorg bevat, maar er op een later moment wellicht nog nadere kwesties aan het licht komen, aangezien het ontwerp-adequaatheidsbesluit nog maar kort geleden werd gepubliceerd.

WP29 erkent dat met het definiëren van het woord "passend" in artikel 25, lid 6, van de richtlijn als "in grote lijnen" overeenkomstig, het HvJEU adequaatheid in de zaak-Schrems nader heeft uitgewerkt. Het Hof heeft benadrukt dat de term "passend beschermingsniveau" niet inhoudt dat het derde land een beschermingsniveau moet waarborgen dat overeenkomt met het niveau dat binnen de rechtsorde van de EU wordt gegarandeerd, maar zo moet worden opgevat dat het derde land, op grond van zijn nationale wetgeving of zijn internationale verbintenissen, een niveau van bescherming van de grondrechten en de fundamentele vrijheden biedt dat *in grote lijnen overeenkomt* met het niveau dat binnen de Unie wordt gewaarborgd op grond van de richtlijn, gelezen in samenhang met het Handvest.

[3] Schrems-arrest, punt 38.
[4] Schrems-arrest, punt 73.

1.1.2 Beoordeling van het commerciële deel van het ontwerp-adequaatheidsbesluit

WP29 heeft reeds in werkdocument 12 ("Doorgifte van persoonsgegevens naar derde landen: toepassing van de artikelen 25 en 26 van de EU-richtlijn betreffende gegevensbescherming") uiteengezet hoe zij de kernbeginselen van de EU-gegevensbescherming heeft toegepast op de doorgifte van persoonsgegevens naar derde landen[5]. WP29 heeft getracht gelijkwaardige waarborgen te vinden die een beschermingsniveau waarborgen dat overeenkomt met de in de richtlijn gegarandeerde beginselen, in het bijzonder met betrekking tot doelbinding, kwaliteit en evenredigheid van gegevens, transparantie, veiligheid, recht op toegang, rectificatie en verweer, gegevensbewaring en beperkingen op verdere doorgifte. Een vergelijkbare werkwijze is gevolgd voor de door WP29 uitgebrachte adviezen ten tijde van de beoordeling van het oorspronkelijke adequaatheidsbesluit[6] met betrekking tot de veiligehavenbeschikking, alsmede voor de aanbevelingen die de werkgroep heeft gedaan in haar op 10 april 2014 gepubliceerde brief aan voormalig vicevoorzitter Viviane Reding, die destijds als Europees commissaris was belast met Justitie[7].

1.1.3 Beoordeling van afwijkingen voor de toegang door overheidsdiensten en de betrokken waarborgen

De beoordeling van de afwijkingen voor de toegang door overheden tot persoonsgegevens die onder het privacyschild vallen, is een complexe opdracht, zeker nu de gegevensbeschermingsautoriteiten en het grote publiek door de onthullingen van Snowden veel beter op de hoogte zijn van toezichtsprogramma's in de VS. Het stemt WP29 tevreden dat de Amerikaanse regering zich inspant om de transparantie met betrekking tot toezichtsprogramma's te vergroten en dat zij bereid is om aanvullende waarborgen in het privacyschild op te nemen. Tegelijkertijd benadrukt WP29 dat elke inperking van de grondrechten betreffende het privéleven en gegevensbescherming in een democratische maatschappij gerechtvaardigd moet kunnen worden. Het HvJEU laakte het feit dat de veiligehavenbeschikking geen bevindingen bevatte over het bestaan, in de Verenigde Staten, van door de staat vastgestelde regels om grenzen te stellen aan elke vorm van inperking. En in de beschikking wordt evenmin verwezen naar het bestaan van doeltreffende wettelijke bescherming tegen een dergelijke inperking[8].

WP29 heeft daarom het huidige rechtskader van de VS en praktijken van Amerikaanse inlichtingendiensten geanalyseerd zoals die worden beschreven in de bijlagen bij het ontwerpbesluit, alsmede de voorwaarden waaronder inperking wordt toegestaan van de krachtens het Europese rechtskader gewaarborgde grondrechten op eerbiediging van het privéleven en gegevensbescherming.

Teneinde te evalueren of een inperking zou kunnen worden gerechtvaardigd in een democratische samenleving, werd de beoordeling uitgevoerd in het licht van de Europese

[5] Vastgesteld door WP29 op 24 juli 1998, zie met name blz. 6.
[6] Zie WP62, WP32, WP27, WP23, WP21, WP19, WP15 en WP7.
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf
[8] Schrems-arrest, punten 87 en 88.

jurisprudentie inzake grondrechten, die vier essentiële waarborgen biedt voor inlichtingenactiviteiten[9]:

A. Verwerking moet stroken met de wet en gebaseerd zijn op duidelijke, exacte en toegankelijke voorschriften; dit betekent dat iedereen die voldoende geïnformeerd is, in staat moet zijn om te voorzien wat er kan gebeuren met zijn gegevens als deze worden doorgegeven;
B. De noodzakelijkheid en evenredigheid van de nagestreefde rechtmatige doelstellingen moeten worden aangetoond: er moet een balans worden gevonden tussen het doel waarvoor de gegevens worden verzameld en waarvoor toegang tot de gegevens wordt verworven, en de rechten van natuurlijke personen;
C. Er moet een onafhankelijk toezichtsmechanisme voorhanden zijn dat zowel doeltreffend als onpartijdig is: dit kan een rechter zijn of een ander onafhankelijk orgaan, zolang het voldoende bekwaam is om de noodzakelijke controles uit te voeren;
D. Natuurlijke personen moeten doeltreffende rechtsmiddelen tot hun beschikking hebben: iedereen moet het recht hebben om zijn rechten ten overstaan van een onafhankelijk orgaan te verdedigen.

1.2 Het ontwerp-adequaatheidsbesluit

WP29 verwelkomt op de eerste plaats het feit dat minder dan zes maanden nadat het HvJEU de veiligehavenbeschikking ongeldig verklaarde, een nieuwe adequaatheidsprocedure kan worden gestart. Met het oog op het grote aantal gegevensdoorgiften dat dagelijks plaatsvindt tussen de EU en de VS, hetgeen WP29 beschouwt als een essentieel onderdeel van de economie aan beide zijden van de Atlantische Oceaan, is zo snel mogelijk juridische duidelijkheid vereist.

WP29 betreurt echter dat het door de Commissie gepubliceerde ontwerp-adequaatheidsbesluit geen uitvoerige beoordeling van de nationale wetgeving en de internationale verbintenissen van de VS omvat in de vorm van een adequaatheidsverslag, zoals in het verleden de normale gang van zaken was bij vergelijkbare procedures en in overeenstemming zou zijn met artikel 25 van de richtlijn. Dit heeft WP29 belet een volledige analyse uit te voeren van de juridische context waarbinnen het privacyschild zal gelden. Zij merkt bijvoorbeeld op dat het huidige ontwerp-adequaatheidsbesluit geen bevindingen omvat over de zowel op federaal als op staatsniveau vigerende wetgeving inzake privacy en gegevensbescherming in de VS, noch inzake sectoriële wetgeving, noch inzake wetgeving die voorziet in andere vormen van openbare toegang dan toezicht. Ook de relatie tussen gegevensdoorgiften op grond van het privacyschild en die op grond van andere bestaande adequaatheidsbevindingen, zoals de EU-VS overeenkomst inzake persoonsgegevens van passagiers (PNR-gegevens) en de overeenkomst inzake het programma voor het traceren van terrorismefinanciering (TFTP), wordt niet beschreven.

[9] De Europese essentiële waarborgen zijn gebaseerd op de jurisprudentie van het HvJEU en het EHRM en worden uitvoeriger beschreven in werkdocument WP237 van WP29, gepubliceerd op 13 april 2016.

1.2.1 Toepassingsgebied van het EU-kader voor gegevensbescherming en, in het bijzonder, van de beginselen van Richtlijn 95/46/EG

WP29 herinnert eraan dat krachtens het EU-rechtskader voor gegevensbescherming, en in het bijzonder volgens de richtlijn (artikel 4, lid 1), de wetgeving van de lidstaten niet alleen van toepassing is op de verwerking die wordt uitgevoerd door op hun grondgebied gevestigde verwerkingsverantwoordelijken, maar ook op gevallen waarin verantwoordelijken voor de gegevensverwerking (hoewel niet gevestigd in de EU) gebruikmaken van apparatuur die zich op het EU-grondgebied bevindt, in het bijzonder voor de verzameling van persoonsgegevens. Bijgevolg is de wetgeving van de EU-lidstaten van toepassing op elke verwerking die plaatsvindt voorafgaand aan de doorgifte aan de VS, ofwel in de context van activiteiten van een in de EU gevestigde organisatie, ofwel doordat een niet in de EU gevestigde organisatie gebruikmaakt van apparatuur die zich in de EU bevindt. WP29 vindt dat dit uitdrukkelijk moet worden gesteld in het ontwerp-adequaatheidsbesluit.

Het zou duidelijk moeten zijn dat de privacyschildbeginselen van kracht zijn vanaf het moment dat de gegevensdoorgifte plaatsvindt. Bovendien herinnert WP29 eraan dat in de EU gevestigde verwerkingsverantwoordelijken die gegevens doorgeven aan een gegevensverwerker in de VS, onderworpen blijven aan de EU-wetgeving inzake gegevensbescherming.

1.2.2 Onvoldoende duidelijkheid in de documenten van het privacyschild

Doordat beginselen en garanties waarin het privacyschild voorziet in zowel het adequaatheidsbesluit als de bijlagen uiteengezet worden, is de informatie moeilijk te vinden en soms onsamenhangend. Dit vergroot de algehele onduidelijkheid met betrekking tot het nieuwe kader en beperkt de toegankelijkheid voor betrokkenen, organisaties en gegevensbeschermingsinstanties. Ook de gebezigde taal is onduidelijk. Daarom verzoekt WP29 de Commissie dringend om er voor te zorgen dat het kader duidelijk en begrijpelijk is voor beide zijden van de Atlantische Oceaan.

WP29 stelt voor om een aparte bijlage op te nemen met gedefinieerde termen die in de documenten van het privacyschild worden gebruikt. Een algemeen en ondubbelzinnig begrip van de bij het adequaatheidsbesluit inzake het privacyschild opgelegde verplichtingen is zeer belangrijk voor een doeltreffende werking ervan aan beide zijden van de Atlantische Oceaan, en WP29 is dan ook bezorgd dat als gevolg van de vele kruisverwijzingen en niet op elkaar afgestemde formuleringen, alsmede door de complexiteit van de kaderdocumenten, bij de tenuitvoerlegging van het privacyschild moeilijkheden zullen ontstaan met betrekking tot de samenhang, begrijpelijkheid en duidelijkheid.

Nog belangrijker is dat in de documenten van het privacyschild terminologie wordt gebezigd die niet consistent is met het begrippenapparaat dat doorgaans in de EU wordt gebruikt met betrekking tot gegevensbescherming. Dit hoeft geen probleem te zijn, zolang duidelijk is hoe de overeenkomstige terminologie binnen de EU-wetgeving (en binnen de Amerikaanse wetgeving) luidt. WP29 betreurt dat dit echter niet het geval is, ook niet met betrekking tot het

ontwerp-adequaatheidsbesluit. Het woord "toegang" wordt bijvoorbeeld in hoofdstuk 3 van het ontwerp-adequaatheidsbesluit zodanig gebruikt dat het verwijst naar verzamelen van persoonsgegevens, in plaats van naar iemand toestaan om gegevens in te zien die reeds verzameld zijn. Toegang door bedrijven tot de gegevens en het recht op toegang van natuurlijke personen zijn twee aparte begrippen, die niet moeten worden verward.

WP29 benadrukt dat de terminologie ook in alle documenten, waaronder het ontwerp-adequaatheidsbesluit, consistent moet worden gebruikt. Dit is momenteel niet het geval, bijvoorbeeld met betrekking tot de begrippen "verwerking" en "persoonsgegevens". Beide zijn in principe goed gedefinieerd in bijlage II, maar worden niet consequent toegepast in alle documenten, hetgeen leidt tot lacunes in de bescherming[10].[11]

WP29 is ingenomen met het feit dat van een aantal gebruikte termen een definitie is opgenomen in de documenten die deel uitmaken van het privacyschild. Dit is echter niet het geval voor een aantal andere essentiële termen, waaronder "vertegenwoordiger" of "verwerker", "gegevens met een unieke code", "geanonimiseerde gegevens" en "natuurlijke persoon uit de EU", die volgens WP29 om een duidelijke definitie vragen, waarover de VS en de EU het eens zijn, teneinde in een later stadium verwarring te voorkomen bij zowel de verwerkingsverantwoordelijken als de verwerkers die het privacyschild gebruiken, de toezichthoudende autoriteiten en het grote publiek. Een gemakkelijke oplossing zou zijn om een verklarende woordenlijst toe te voegen aan de FAQ van het privacyschild.

WP29 wijst ook op de geldige redenen voor het verwerken van gevoelige gegevens in aanvullend beginsel 1 (bijlage II, punt III.1), in gevallen waarbij een organisatie geen expliciete toestemming hoeft te verkrijgen (opt-in). Aanvullend beginsel 1 kan worden gezien als een gedetailleerde beschrijving van de geldige redenen voor het verzamelen van gegevens in de EU, aangezien deze lijst vergelijkbaar is met artikel 8 van de richtlijn. WP29 wil er graag op wijzen dat elke verwerking (inclusief verzameling en doorgifte) van gevoelige gegevens die onder het EU-recht valt, volgens artikel 8 van de richtlijn moet plaatsvinden op grond van geldige redenen. Het privacyschild kan niet zodanig worden uitgelegd dat het

[10] Sommige bepalingen bevatten slechts een opsomming van enkele vormen van gegevensverwerkingsactiviteiten, zonder vermelding van de term "verwerking". Dit leidt tot lacunes in de bescherming. Volgens de formulering van bijlage II, punt III.6.f, zouden de privacyschildbeginselen bijvoorbeeld alleen van toepassing zijn wanneer de organisatie de ontvangen gegevens "opslaat, gebruikt of openbaar maakt" (d.w.z. niet voor andere diensten die onder de term "verwerking" vallen, zoals verzamelen, vastleggen, wijzigen, opvragen, raadplegen, wissen). Gegevensbeveiliging zou alleen worden opgelegd voor het "creëren, bewaren, gebruiken of verspreiden" van persoonsgegevens (bijlage II, punt II.4). De definitie van persoonsgegevens is ook beperkt tot "ontvangen" en "geregistreerde" gegevens. Een ander voorbeeld is dat volgens het kennisgevingsbeginsel (bijlage II, punt II.1.a.iv) de gecertificeerde organisatie natuurlijke personen moet informeren over het doel waarvoor zij gegevens over hen "verzamelt en gebruikt". Bijlage II, punt III.9.a.ii, noemt alleen gegevens die zijn "doorgegeven of toegankelijk worden gemaakt". Hoewel het in de meeste gevallen niet de bedoeling lijkt om het toepassingsgebied van de beginselen te beperken of om lacunes in de bescherming te creëren, brengt deze inconsistente terminologie het risico mee dat dergelijke lacunes worden veroorzaakt. Aangezien de term "verwerking" in de beginselen wordt gedefinieerd, is het uitermate belangrijk om deze op consistente wijze te hanteren teneinde de huidige lacunes te voorkomen. Anders zou er te veel ruimte worden gelaten voor vermoedelijk niet-beoogde uitleggingen, die zouden kunnen leiden tot een verkeerde interpretatie van de bewoordingen van het besluit.

[11] De in bijlage II, punt I.8.a, opgenomen definitie van "persoonsgegevens" verwijst naar "gegevens over een geïdentificeerde of identificeerbare natuurlijke persoon". Het aanvullend beginsel bepaalt echter dat de beginselen met betrekking tot personeelsgegevens alleen van toepassing zijn als "bestanden over individueel bepaalde personen worden doorgegeven of toegankelijk worden gemaakt". WP29 is van mening dat dit de mogelijkheid biedt om persoonsgegevens te verwerken op een manier die niet in overeenstemming is met de gegevensbeschermingsbeginselen krachtens het EU-recht, en ook niet met de algemene definitie van persoonsgegevens uit hoofde van het privacyschild.

voorziet in alternatieve redenen voor dergelijke verwerking. Volgens WP29 is het voor een organisatie in de VS bijvoorbeeld niet mogelijk om aan EU-recht onderworpen gegevens te verzamelen op basis van het Amerikaanse arbeidsrecht (zie bijlage II, punt III.1.a.v). Daarom benadrukt WP29 dat elke interpretatie van aanvullend beginsel 1 alleen mag leiden tot de toepassing ervan op gevoelige gegevens die al zijn doorgegeven nadat ze in de EU zijn verzameld op grond van de in artikel 8 van de richtlijn vermelde geldige redenen.

WP29 stelt ten slotte vast dat onduidelijk is wie als natuurlijke persoon uit de EU moet worden beschouwd en dus profiteert van bescherming uit hoofde van het privacyschild: alle EU-burgers of alle personen die in de EU verblijven. Dit is in het bijzonder van belang met betrekking tot het verhaalsrecht, inclusief de toegang tot het mechanisme van de ombudsman. Bovendien moet het adequaatheidsbesluit antwoord geven op de vraag in hoeverre het privacyschild ook van toepassing zal zijn op burgers/ingezetenen van de landen van de EER en Zwitserland, die in het verleden onder de veiligehavenregeling vielen.

1.2.3 Gezamenlijke evaluatie en opschorting

WP29 is verheugd over het feit dat de Europese Commissie en de Amerikaanse regering overeengekomen zijn om de praktische toepassing van het privacyschild regelmatig te evalueren. Deze gezamenlijke evaluatie is al een aantal jaren een bekende praktijk bij degenen die in de EU bij gegevensbescherming betrokken zijn, in het bijzonder met betrekking tot de overeenkomsten inzake de uitwisseling van PNR-gegevens met derde landen en de TFTP-overeenkomst. WP29 is bovendien verheugd over het feit dat een onbepaald aantal vertegenwoordigers van gegevensbeschermingsautoriteiten kan deelnemen aan deze gezamenlijke evaluaties.

Gezien haar ervaring met gezamenlijke evaluaties van de laatste jaren, wil WP29 graag duidelijk maken dat zij verwacht dat de gezamenlijke evaluatie van het privacyschild uitgebreider zal zijn dan de gezamenlijke evaluaties van de PBR en TFTP. Het is met name wenselijk dat de gezamenlijke evaluatie niet alleen bijeenkomsten omvat met vertegenwoordigers van agentschappen, organisaties en bedrijven uit de VS, maar ook verificaties ter plaatse van bepaalde onderdelen van het privacyschild. De bij de gezamenlijke evaluatie betrokken vertegenwoordigers van de gegevensbeschermingsautoriteiten moeten voorstellen kunnen indienen voor dergelijke verificaties ter plaatse.

WP29 is van mening dat voor een gezamenlijke evaluatie een gezamenlijke beoordeling van de bevindingen noodzakelijk is. Tot nu toe worden de resultaten van gezamenlijke evaluaties gepresenteerd in een document van de diensten van de Commissie, waarvoor geen goedkeuring vereist was van de leden van het gezamenlijke-evaluatieteam die niet in dienst zijn van de Commissie. Voor de gezamenlijke evaluatie van het privacyschild zou WP29 het op prijs stellen als het verslag met de bevindingen inderdaad een gemeenschappelijk product zou kunnen zijn. Als alternatief zou kunnen worden overwogen om de gegevensbeschermingsautoriteiten een afzonderlijk verslag van de gezamenlijke evaluatie te laten uitbrengen.

Ten slotte wijst WP29 ten aanzien van de gezamenlijke evaluatie op de toezegging van de Commissie dat de kosten die de vertegenwoordigers van WP29 tijdens gezamenlijke evaluaties maken, door de Commissie zullen worden vergoed. De werkgroep neemt aan dat dit ook geldt voor de gezamenlijke evaluatie van het privacyschild, in elk geval voor een redelijk aantal vertegenwoordigers van gegevensbeschermingsautoriteiten.

WP29 adviseert dat uiterlijk drie maanden voordat de eerste gezamenlijke evaluatie van het privacyschild zou moeten plaatsvinden, de regeling voor de gezamenlijke evaluatie in overleg tussen de Commissie, de Amerikaanse regering en WP29 overeengekomen en schriftelijk vastgelegd worden.

1.2.4 Het EU-rechtskader wordt momenteel herzien

Het adequaatheidsbesluit inzake het privacyschild is het eerste adequaatheidsbesluit dat is opgesteld na de principeovereenkomst over de tekst van de algemene verordening gegevensbescherming. WP29 heeft echter vastgesteld dat het privacyschild nog niet aansluit bij de toekomstige situatie. Zo zijn belangrijke nieuwe begrippen, zoals het recht op gegevensoverdraagbaarheid, en aanvullende verplichtingen van de verwerkingsverantwoordelijken, inclusief de behoefte om effectbeoordelingen met betrekking tot gegevensbescherming uit te voeren en te voldoen aan de beginselen van "privacy by design" ("ingebouwde privacy") en "privacy by default" ("standaard-privacy"), bijvoorbeeld niet opgenomen in het privacyschild. WP29 zou daarom willen voorstellen om het privacyschild, zoals alle bestaande adequaatheidsbesluiten, te evalueren, kort nadat de algemene verordening gegevensbescherming van toepassing wordt. Een uitdrukkelijke verwijzing naar deze evaluatie in het definitieve adequaatheidsbesluit zou op prijs worden gesteld.

2. BEOORDELING VAN HET COMMERCIËLE DEEL VAN HET ONTWERP-ADEQUAATHEIDSBESLUIT

2.1 Algemene opmerkingen

2.1.1 Verbeteringen

WP29 verwelkomt de verbeteringen die het privacyschild meebrengt en de bereidheid van de onderhandelaars om de door haar benadrukte tekortkomingen van de veilige haven aan te pakken. Ten opzichte van de veilige haven, hebben de verbeteringen met name betrekking op de volgende onderdelen: de definiëring van belangrijke begrippen als "persoonsgegevens", "verwerking" en "verwerkingsverantwoordelijke", de mechanismen die zijn ingesteld om het toezicht op de privacyschildlijst te waarborgen en de nu verplichte externe dan wel interne nalevingscontroles. Ook het toegangsbeginsel wordt verbeterd en WP29 merkt op dat de rechten op verbetering en verwijdering nu gelden als gegevens worden gebruikt op een manier die onverenigbaar is met de beginselen van het privacyschild. Bovendien wordt nu duidelijk gemaakt dat de natuurlijke persoon een bevestiging moet ontvangen dat gegevens

over hem worden verwerkt, maar dat hem ook moet worden meegedeeld om welke gegevens het gaat.

WP29 is tevens verheugd over de versterking van de juridische garanties die gelden bij verdere doorgifte, en over de toezeggingen van het DoC en de Amerikaanse Federal Trade Commission (FTC) om toe te zien op de naleving van de in het privacyschild vastgestelde verplichtingen.

2.1.2 Toepassing van het privacyschild op organisaties die optreden als verwerker (vertegenwoordiger)

In hoeverre de beginselen van het privacyschild van toepassing zijn op gecertificeerde organisaties die persoonsgegevens van de EU uitsluitend voor verwerkingsdoeleinden ontvangen (hierna te noemen "vertegenwoordigers" of "verwerkers"), blijft helaas onduidelijk. Hoewel in de bepalingen in bijlage II, punt III.10.a, gegevensdoorgifte naar gecertificeerde organisaties voor dergelijke doeleinden wordt vermeld – althans de vereiste om een overeenkomst te sluiten is opgenomen – bevatten ze geen enkele aanwijzing over de wijze waarop de beginselen van het privacyschild van toepassing zijn op verwerkers (vertegenwoordigers). Dit veroorzaakt onduidelijkheid, zowel voor de gecertificeerde organisaties in de VS die gegevens ontvangen voor verwerkingsdoeleinden en de bedrijven in de EU die gegevens doorgeven aan gecertificeerde organisaties die optreden als gegevensverwerkers, als voor de natuurlijke personen wier gegevens worden verwerkt. Hierdoor zal het moeilijk vast te stellen zijn welke verplichtingen daadwerkelijk gelden voor privacyschildorganisaties die als verwerker uit de EU ontvangen persoonsgegevens verwerken. Opheldering is daarom zeker vereist.

In aanmerking moet worden genomen dat een aantal in de beginselen opgenomen verplichtingen niet geschikt is voor gegevensverwerkers, omdat de doeleinden en middelen voor het verwerken van de gegevens altijd worden vastgesteld door de verwerkingsverantwoordelijke (zie de definitie van "verwerkingsverantwoordelijke" in bijlage II, punt I.8.c). Daardoor kunnen bepaalde in de beginselen opgenomen verplichtingen, indien toegepast op een organisatie die optreedt als vertegenwoordiger, strijdig zijn met de gegevensverwerkingsovereenkomst die vereist is krachtens EU-recht (de overeenkomst genoemd in bijlage II, punt III.10.a). Zo staat de gegevensverwerkingsovereenkomst de gegevensverwerker (vertegenwoordiger) over het algemeen de verdere doorgifte van gegevens naar een derde verwerkingsverantwoordelijke niet toe, zelfs niet onder de genoemde omstandigheden in bijlage II, punt II.3.a. Verdere doorgifte naar derde vertegenwoordigers dient uitsluitend te worden toegestaan na voorafgaande goedkeuring van de verwerkingsverantwoordelijke. Bovendien kan een verwerker (vertegenwoordiger) volgens de vereisten van het EU-recht natuurlijke personen geen volledige kennisgeving verschaffen in de zin van het kennisgevingsbeginsel (bijlage II, punt II.1), bijvoorbeeld omdat deze organisatie de doelen van de verwerking niet vaststelt.

Het is daarom heel belangrijk om in de beginselen duidelijk te maken dat in het geval van een dergelijke tegenstrijdigheid de bepalingen van de gegevensverwerkingsovereenkomst zullen

gelden, en in het bijzonder de instructies van de organisatie die de gegevens vanuit de EU doorgeeft. Zonder deze opheldering zouden de beginselen kunnen worden uitgelegd en toegepast op een manier die de privacyschildvertegenwoordiger te veel controlebevoegdheden geeft, hetgeen voor de gegevensexporteur van de EU het risico zou meebrengen dat hij zijn verplichtingen als verwerkingsverantwoordelijke krachtens de EU-wetgeving inzake gegevensbescherming schendt, waaraan hij is onderworpen als hij gegevens doorgeeft aan een privacyschildorganisatie die optreedt als vertegenwoordiger. Bovendien wekt dit gebrek aan duidelijkheid de indruk dat de verwerker de gegevens naar wens opnieuw kan gebruiken.

Voorts moet worden voorzien in specifieke voorschriften voor het geval een organisatie als gegevensverwerker (vertegenwoordiger) optreedt, om ervoor te zorgen dat deze organisatie de instructies van de verwerkingsverantwoordelijke naleeft. Duidelijk moet worden gemaakt dat Amerikaanse organisaties die gegevens uitsluitend voor verwerkingsdoeleinden ontvangen, niet zelf mogen beslissen om de gegevens te verwerken. Zonder specifieke voorschriften voor organisaties die als verwerker optreden, is het moeilijk om vast te stellen op grond van welke voorschriften de verwerker (vertegenwoordiger) zichzelf zou kunnen certificeren.

2.1.3 Beperkingen van de verplichting zich aan de beginselen te houden

Bijlage II, punt I.5, voorziet onder andere in vrijstellingen van de beginselen ingeval gegevens die onder het privacyschild vallen, worden gebruikt om te voldoen aan vereisten inzake nationale veiligheid[12], het algemeen belang of rechtshandhaving, dan wel op grond van de wet, overheidsreglementering of jurisprudentie die tegenstrijdige verplichtingen of uitdrukkelijke bevoegdheden creëert. Zonder volledige kennis van het Amerikaanse recht op zowel federaal als staatsniveau, is het voor WP29 moeilijk om de reikwijdte van deze vrijstelling vast te stellen en om te beoordelen of deze beperkingen in een democratische maatschappij gerechtvaardigd zijn. Het is essentieel dat de Europese Commissie in haar ontwerp-adequaatheidsbesluit ook een analyse opneemt van het beschermingsniveau dat wordt geboden wanneer deze vrijstellingen van toepassing zijn. WP29 verzoekt de Commissie om te waarborgen dat de EU wordt geïnformeerd over elke wet of overheidsreglementering die gevolgen zou kunnen hebben voor de naleving van de beginselen. Dit geldt zowel voor de vigerende wetten en regels als om instrumenten die in de toekomst in de VS van kracht worden.

2.1.4 Ontbreken van een beperkingsbeginsel voor gegevensbewaring

Het beperkingsbeginsel voor gegevensbewaring (artikel 6, lid 1, onder e), van de richtlijn) is een fundamenteel beginsel in het EU-gegevensbeschermingsrecht, dat voorschrijft dat persoonsgegevens niet langer mogen worden bewaard dan nodig is voor de verwezenlijking van de doeleinden waarvoor de gegevens worden verzameld of waarvoor ze vervolgens worden verwerkt.

[12] Zie hoofdstuk 3 voor verdere toelichting over het gebruik van onder het privacyschild vallende persoonsgegevens ten behoeve van de nationale veiligheid en hoofdstuk 4 voor wetshandhavingsdoeleinden.

WP29 kan uit de documenten die deel uitmaken van het privacyschild echter niet opmaken dat de gegevensverwerkingsverantwoordelijken moeten waarborgen dat de gegevens worden verwijderd als het doeleinde waarvoor ze werden verzameld of nader verwerkt, niet meer relevant is. Het lijkt er dus op dat wat betreft de duur van het bewaren van de gegevens de gecertificeerde organisaties krachtens de beginselen niet gehouden zijn aan een limiet die vergelijkbaar is met de termijn die volgt uit het in het EU-recht vervatte beperkingsbeginsel voor gegevensbewaring.

De beginselen van gegevensintegriteit en doelbinding (bijlage II, punt II.5) zij zo geformuleerd, dat ze in geen geval zo kunnen worden opgevat dat een organisatie die optreedt als verwerkingsverantwoordelijke, ertoe verplicht zou zijn gegevens te verwijderen wanneer die niet langer nodig zijn voor de doeleinden waarvoor de gegevens werden verzameld of vervolgens verwerkt, of dat een organisatie die optreedt als een verwerker, ertoe verplicht zou zijn gegevens te verwijderen na de beëindiging van de dienstenovereenkomst.

De werkgroep onderstreept dat het ontbreken van bepalingen die een limiet stellen aan de bewaring van gegevens die onder het privacyschild vallen, organisaties de mogelijkheid geeft om gegevens net zo lang te bewaren als zij willen, zelfs als de gegevens niet meer onder het privacyschild vallen, wat niet in overeenstemming is met het beperkingsbeginsel voor gegevensbewaring.

2.1.5 Ontbreken van waarborgen voor geautomatiseerde besluiten die rechtsgevolgen teweegbrengen of aanzienlijke gevolgen hebben voor de natuurlijke persoon

Het privacyschild voorziet niet in juridische garanties wanneer natuurlijke personen worden onderworpen aan een besluit dat tot rechtsgevolgen leidt die hen betreffen of die aanzienlijke gevolgen voor hen meebrengen, en dat louter wordt genomen op grond van geautomatiseerde gegevensverwerking voor de evaluatie van bepaalde persoonlijke kenmerken, zoals prestaties op het werk, kredietwaardigheid, betrouwbaarheid, gedrag, enz.

De noodzaak om juridische garanties te verschaffen voor geautomatiseerde besluiten (die rechtsgevolgen teweegbrengen of aanzienlijke gevolgen hebben voor de natuurlijke persoon) teneinde een passend beschermingsniveau te verschaffen, werd reeds in werkdocument 12 door WP29 onderstreept.

Dit is des te noodzakelijker doordat dankzij de voortdurend evoluerende nieuwe technologieën meer bedrijven kunnen overwegen om te werken met geautomatiseerde besluitvormingssystemen, die kunnen leiden tot een verzwakking van de positie van natuurlijke personen, voor zover deze geen verhaal meer kunnen instellen tegen deze door de computer genomen besluiten. Wanneer besluiten die volledig door deze geautomatiseerde systemen worden genomen, gevolgen hebben voor de rechtspositie van natuurlijke personen of andere aanzienlijke gevolgen voor hen hebben (bijvoorbeeld doordat natuurlijke personen op een zwarte lijst worden geplaatst en zodoende van hun rechten worden beroofd), is het belangrijk om voldoende waarborgen te bieden, waaronder het recht om de achterliggende

redenering te kennen en het recht om te verzoeken om heroverweging op een niet-geautomatiseerde basis.

2.1.6 Overgangsperiode voor bestaande handelsbetrekkingen

Het privacyschild bepaalt dat de beginselen onmiddellijk na certificering van kracht worden. Organisaties die certificeren in de eerste twee maanden nadat het kader van het privacyschild van kracht wordt, moeten echter alle bestaande handelsbetrekkingen met derde partijen zo snel mogelijk in overeenstemming brengen met het beginsel van verantwoording voor verdere doorgifte. In elk geval moet dit plaatsvinden binnen negen maanden na de datum van certificering voor het privacyschild.

Dit betekent dat bestaande overeenkomsten indien nodig tussen twee en negen maanden na de certificering in overeenstemming moeten worden gebracht met de beginselen. Gedurende deze overgangsperiode volstaan de beginselen van kennisgeving en keuze. WP29 beklemtoont dat doorgiften pas op basis van het privacyschild kunnen plaatsvinden wanneer de organisatie volledig aan alle vereisten van het schild kan voldoen. De mogelijkheid om tijdens een overgangsperiode gegevens te versturen zonder dat de ontvanger volledig aan de beginselen van het schild kan voldoen, strookt niet met de voorwaarden voor wettelijke doorgifte en is niet acceptabel.

2.2 Specifieke opmerkingen

2.2.1 Transparantie

a) Algemene opmerkingen met betrekking tot kennisgeving

WP29 is verheugd over de uitvoerige en gedetailleerde vereisten die zijn vervat in het kennisgevingsbeginsel , en in het bijzonder over het feit dat de kennisgeving een link naar of een adres van een website met de privacyschildlijst dient te omvatten en zowel het toegangsrecht van burgers als de mechanismen voor alternatieve geschillenbeslechting dient te vermelden[13]. WP29 stelt echter voor om duidelijker te zijn over de andere rechten (corrigeren of verwijderen indien onjuist of in strijd met de beginselen verwerkt) waarin wordt voorzien.

De documenten die deel uitmaken van het privacyschild zijn reden tot zorg wat betreft de termijn waarbinnen een privacyschildorganisatie een natuurlijke persoon in kennis moet stellen. In bijlage II, punt II.1.b, is bepaald dat een "kennisgeving (...) in duidelijke en ondubbelzinnige bewoordingen [moet] worden gedaan als de betrokkenen voor de eerste keer wordt gevraagd de organisatie persoonlijke informatie te verstrekken of zo spoedig mogelijk daarna, maar in ieder geval voordat de organisatie dergelijke informatie gebruikt voor een ander doel dan waarvoor deze oorspronkelijk is verzameld of door de doorgevende organisatie is verwerkt, of voor de eerste keer aan een derde bekendmaakt". WP29 is van mening dat in veel situaties een Amerikaanse schildorganisatie niet rechtstreeks gegevens

[13] Bijlage II, punt II.1; WP29 verwijst ook naar de tweede aanbeveling van de Commissie in Mededeling COM(2103) 847 alsmede naar de brief van WP29 aan vicevoorzitter Reding van 10 april 2014, in het bijzonder punt 4, onder "Transparantie".

verzamelt van de betrokkene en dat de kennisgeving derhalve moet plaatsvinden op het moment dat de gegevens door de schildorganisatie worden geregistreerd.

WP29 merkt op dat de concrete toepassing van de vereisten inzake het kennisgevingsbeginsel en het privacybeleid moet worden beoordeeld bij de eerste jaarlijkse evaluatie van het privacyschild.

b) Openbaarheid van het privacybeleid

WP29 is verheugd over het feit dat nu duidelijk is dat het DoC zal controleren of bedrijven die een openbare website hebben, hun privacybeleid op deze website hebben bekendgemaakt of, als ze geen openbare website hebben, waar het privacybeleid openbaar wordt gemaakt[14].

c) Publicatie van privacyvoorwaarden van overeenkomsten met verwerkers

Het privacyschild voorziet, in het kader van de voorwaarden waaronder privacyschildorganisaties gegevens kunnen doorgeven aan een verwerker (vertegenwoordiger), in een verplichting voor zelfcertificerende organisaties om "aan het ministerie op verzoek een samenvatting of een betrouwbare kopie over [te] leggen van de relevante privacybepalingen van de overeenkomst met die vertegenwoordiger" (zie bijlage II, punt II.3.b.vi). De werkgroep verwelkomt deze vereiste om transparantie te betrachten tegenover het DoC.

2.2.2 Keuzemogelijkheden

Het privacyschild voorziet in het recht op verzet (opt-out) tegen de bekendmaking van persoonlijke informatie aan een derde en tegen het gebruik van persoonlijke informatie voor een wezenlijk ander doeleinde[15] (bijlage II, punt III.2). Bovendien kunnen burgers zich te allen tijde verzetten tegen het gebruik van persoonlijke informatie voor directmarketingdoeleinden (bijlage II, punt III.12.a)[16].

Behalve in de context van directmarketingactiviteiten wordt geen nadere informatie verschaft over de wijze en het moment waarop deze “opt-out” kan worden uitgeoefend. WP29 is van mening dat het niet voldoende is om slechts in het privacybeleid naar het bestaan van dit recht te verwijzen, maar dat er voordat persoonlijke informatie openbaar wordt gemaakt of wordt hergebruikt een geïndividualiseerde mogelijkheid moet worden geboden om dit recht uit te oefenen.

Bovendien benadrukt WP29 dat een algemeen recht om bezwaar te maken (om zwaarwegende redenen in verband met de specifieke situatie van de betrokkene), opgevat als het recht om beëindiging te vragen van de verwerking van de gegevens wanneer de persoon zwaarwegende gerechtvaardigde redenen heeft met betrekking tot deze specifieke situatie,

[14] Zie de eerste aanbeveling van de Europese Commissie in mededeling COM(2013) 847 en de brief van 10 april 2014 van WP29 aan vicevoorzitter Reding, in het bijzonder punt 3 onder "Transparantie".
[15] Het aanvullend beginsel 14.c.I voorziet in het recht om zich terug te trekken uit een klinisch onderzoek, hetgeen kan worden gezien als het recht om bezwaar te maken of gegeven toestemming in te trekken.
[16] Dit is identiek aan het bepaalde in de veiligehavenregeling (FAQ 12) en er is in dit opzicht geen wijziging aangebracht.

moet worden geboden binnen het privacyschild[17]. WP29 adviseert met klem dat het ontwerp-adequaatheidsbesluit duidelijk maakt dat het recht om bezwaar te maken op elk moment beschikbaar moet zijn, en dat dit bezwaar niet beperkt is tot het gebruik van de gegevens voor direct marketing[18].

WP29 vreest dat het ontbreken van een omschrijving van wat als een "materieel verschillend" doel moet worden beschouwd, tot verwarring en rechtsonzekerheid zal leiden. Het moet in elk geval duidelijk worden gemaakt dat het keuzebeginsel niet kan worden gebruikt om het doelbindingsbeginsel te omzeilen[19]. Keuzemogelijkheden moeten alleen toepasselijk zijn wanneer het doeleinde materieel verschillend, maar toch verenigbaar is, aangezien de verwerking voor onverenigbare doeleinden verboden is (bijlage II, punt II.5.a). Het moet duidelijk worden gemaakt dat het recht op verzet de organisatie niet in staat kan stellen om gegevens te gebruiken voor onverenigbare doeleinden. Daarom beveelt WP29 aan om de betreffende formulering te harmoniseren door gebruik te maken van één enkele gedefinieerde formulering (bijv. een "materieel verschillend, maar toch verenigbaar doel").

Verduidelijking zou nuttig zijn met betrekking tot de vraag of een besluit om gegevens te verwerken voor een ander doel of om informatie bekend te maken, onder het EU-recht valt. In deze situatie zullen de gebruikelijke juridische voorwaarden van de EU met betrekking tot deze verwerking (zoals het verbod op verwerking voor onverenigbare doeleinden, het verschaffen van een rechtmatige reden voor de verwerking en de noodzaak om de persoon te informeren) rechtstreeks van toepassing zijn, ook op de Amerikaanse organisatie die onder de werkingssfeer van het EU-recht valt. In de praktijk komt dit erop neer dat de EU-exporteur die een dergelijk besluit neemt, de transparantie en wettigheid van de verwerking volgens het EU-recht moet waarborgen. Daarom zal het keuzebeginsel alleen van toepassing zijn wanneer het besluit uitsluitend door een niet aan het EU-recht onderworpen schildorganisatie in de VS wordt genomen.

2.2.3 Verdere doorgifte

a) Toepassingsgebied

WP29 maakt zich zorgen over de situatie waarbij verdere doorgiften van persoonsgegevens plaatsvinden van een door het privacyschild gecertificeerde organisatie in de VS naar een ontvanger in een derde land.

Het schild moet niet alleen worden beschouwd als een middel om EU-gegevens van de EU naar de VS door te geven, maar zal ook dienen als een middel om gegevens van de VS naar derde landen door te geven. Bepalingen over verdere doorgifte zijn daarom een belangrijk onderdeel van het schild en moeten voldoende garanties en een passend beschermingsniveau

[18] Zie de brief van WP29 aan vicevoorzitter Reding, onder "Choice".
[19] Een concreet voorbeeld van verdere onverenigbare verwerking die volgens het keuzebeginsel is toegestaan, is opgenomen onder aanvullend beginsel 9.b.i (zie het commentaar van WP29 daarover onder het punt "Verwerking van personeelsgegevens").

bieden wanneer gegevens vanuit de VS verder worden doorgegeven. Eén specifieke kwestie houdt verband met nationale veiligheid en rechtshandhaving.

Het beginsel van verantwoording voor verdere doorgifte op grond van het privacyschild is niet beperkt tot in de VS gevestigde verwerkingsverantwoordelijken, verwerkers of vertegenwoordigers die gegevens ontvangen. Daarom zouden op basis van het privacyschild doorgiften naar een derde land kunnen plaatsvinden, zelfs als het derde land wetgeving heeft die voorziet in openbare toegang tot persoonsgegevens, bijvoorbeeld voor toezichtdoeleinden. Hierdoor worden EU-gegevens blootgesteld aan het risico van ongerechtvaardigde inbreuken op de bescherming van de grondrechten.

Bij elke verdere doorgifte naar een derde land moet elke privacyschildorganisatie verplicht zijn om voorafgaand aan de doorgifte de bindende vereisten van de nationale wetgeving van het derde land en die van toepassing zijn op gegevensimporteurs, te beoordelen. Als wordt vastgesteld dat er een risico bestaat op aanzienlijk nadelige gevolgen voor door het privacyschild verschafte garanties, verplichtingen en beschermingsniveaus, moet de Amerikaanse privacyschildorganisatie die optreedt als verwerker (vertegenwoordiger) de verwerkingsverantwoordelijke van de EU onmiddellijk op de hoogte stellen voordat hij een doorgifte uitvoert. In deze gevallen heeft de gegevensexporteur het recht om de doorgifte van gegevens op te schorten en/of de overeenkomst op te zeggen. Indien er sprake is van een dergelijk risico op aanzienlijk nadelige gevolgen mag een als verwerkingsverantwoordelijke optredende privacyschildorganisatie de gegevens niet doorgeven, omdat dit haar verplichting om in een beschermingsniveau te voorzien dat gelijk is aan dat volgens de beginselen bij verdere doorgifte in gevaar zou brengen (zie bijlage II, punt II.3.a).

Evenzo moet de als verwerker (vertegenwoordiger) optredende privacyschildorganisatie, bij een wijziging van de wetgeving van het derde land die waarschijnlijk een aanzienlijk nadelig effect heeft op de door het privacyschild geboden garanties, verplichtingen en beschermingsniveau, op grond van het privacyschild worden verplicht om, zodra hij van die wijziging kennisneemt, onmiddellijk de gegevensexporteur in kennis te stellen van de wijziging, waarna de gegevensexporteur het recht heeft om de doorgifte van gegevens op te schorten en/of de overeenkomst op te zeggen. In een dergelijk geval moet een als verwerkingsverantwoordelijke optredende privacyschildorganisatie geen toestemming krijgen voor doorgifte, omdat zij verplicht is hetzelfde beschermingsniveau te bieden als volgens de beginselen (zie bijlage II, punt II.3.a).

WP29 brengt haar standpunt in herinnering dat indien de EU-verwerkingsverantwoordelijke, zelfs voordat de doorgifte naar de VS plaatsvindt, op de hoogte is van een verdere doorgifte naar een derde buiten de VS, of indien de EU-verwerkingsverantwoordelijke gezamenlijk verantwoordelijk is voor het besluit om verdere doorgifte toe te staan, de doorgifte beschouwd moet worden als een rechtstreekse doorgifte van de EU naar het derde land buiten de VS. Dit betekent dat op de doorgifte de artikelen 25 en 26 van de richtlijn van toepassing zijn, in plaats van het beginsel van verdere doorgifte in het kader van het privacyschild.

b) Doorgifte van een privacyschildorganisatie naar een derde verwerkingsverantwoordelijke

WP29 is verheugd over de verplichting om een overeenkomst op te stellen (bijlage II, punt II.3.a) die waarborgt dat een derde verwerkingsverantwoordelijke ten minste hetzelfde niveau van privacybescherming biedt als het niveau dat de privacyschildbeginselen vereisen. Het doel daarvan is te waarborgen dat persoonsgegevens adequaat beschermd blijven, ook nadat deze verder zijn doorgegeven. WP29 heeft echter enkele opmerkingen over de voorgestelde voorwaarden.

Geen duidelijke verwijzing naar het doelbindingsbeginsel

WP29 adviseert ook om een duidelijke verwijzing naar het doelbindingsbeginsel (bijlage II, punt II.5) op te nemen binnen de voorwaarden voor verdere doorgiften naar een derde verwerkingsverantwoordelijke (bijlage II, punt II.3.a). Dit zou duidelijk maken dat verdere doorgiften niet mogen plaatsvinden wanneer de derde verwerkingsverantwoordelijke gegevens verwerkt voor een onverenigbaar doel.

Vrijstelling van de verplichte overeenkomst voor doorgiften binnen groepen verwerkingsverantwoordelijken

Er wordt voorzien in een vrijstelling van de verplichte overeenkomst voor doorgiften binnen groepen verwerkingsverantwoordelijken. In een dergelijk scenario kan volgens de beginselen de continuïteit van de bescherming worden gewaarborgd door bindende bedrijfsvoorschriften (*binding corporate rules*, BCR) of "andere intragroepsinstrumenten (bv. nalevings- en controleprogramma's)" (bijlage II, punt III.10.b). WP29 is van mening dat de verwijzing naar "andere intragroepsinstrumenten" niet garandeert dat de andere leden van de groep wettelijk bindende toezeggingen hebben gedaan. Aangezien WP29 en de wetgeving van de EU[20] over het algemeen de voorkeur gegeven aan bindende toezeggingen om doorgiften binnen een groep te regelen, is het belangrijk te voorkomen dat het privacyschild wordt gebruikt om deze eis te omzeilen. WP29 brengt in herinnering dat verdere doorgiften van de VS naar derde landen die al gepland zijn voordat de doorgifte naar de VS heeft plaatsgevonden, of die onderworpen zijn aan gezamenlijke verwerkingsverantwoordelijkheid met de verwerkingsverantwoordelijke in de EU[21], moeten worden beschouwd als rechtstreekse doorgifte van de EU naar het derde land buiten de VS. De artikelen 25 en 26 van de richtlijn zijn daarom van toepassing op de doorgifte.

c) Doorgiften van een privacyschildorganisatie naar een derde verwerker (vertegenwoordiger)

WP29 is verheugd over het feit dat een overeenkomst voor verdere doorgiften nu verplicht is voor ontvangende entiteiten die optreden als verwerkers (vertegenwoordigers), ongeacht hun deelname aan het privacyschild en ongeacht of zij profiteren van een andere oplossing voor het vaststellen van adequaatheid. WP29 is ook verheugd over de aanvullende waarborgen die

[20] De noodzaak van bindende en afdwingbare verbintenissen wordt ook onderstreept in de algemene verordening gegevensbescherming, ongeacht het gebruikte instrument (BCR's, contractuele bepalingen, gedragscodes of certificering).
[21] Bijvoorbeeld voor personeelsgegevens.

voor deze verdere doorgiften gelden (bijlage II, punten II.3.a.1, II.3.a.iii, II.3.a.iv, II.3.a.v en II.7.d). Het laatste punt (bijlage II, punt II.7.d) betreft de verplichting om aansprakelijk te blijven als gegevens bekend worden gemaakt aan een vertegenwoordiger. Het lijkt er echter op dat deze garantie niet van toepassing is wanneer een organisatie ervoor heeft gekozen om samen te werken met een gegevensbeschermingsautoriteit (zie bijlage II, punt III.5.a in fine). WP29 begrijpt de reden voor deze vrijstelling niet en is van mening dat de aansprakelijkheid ook in dat geval moet gelden.

Geen duidelijke verwijzing naar het doelbindingsbeginsel

WP29 merkt op dat in het beginsel van verantwoording voor verdere doorgifte (bijlage II, punt II.3) uiteengezet wordt dat persoonsgegevens uitsluitend voor beperkte en welomschreven doeleinden kunnen worden doorgegeven aan een als vertegenwoordiger handelende derde, maar vermeldt niet uitdrukkelijk dat deze beperkte en welomschreven doeleinden verenigbaar moeten zijn met de oorspronkelijke doeleinden waarvoor de gegevens werden verzameld en met de instructies van de verwerkingsverantwoordelijke. Er is meer duidelijkheid nodig op dit punt. WP29 stelt dan ook voor om ervoor te zorgen dat dit punt in het adequaatheidsbesluit nader wordt gespecificeerd, bijvoorbeeld door het opnemen van een duidelijke verwijzing naar het doelbindingsbeginsel (bijlage II, punt II.5), welk beginsel inhoudt dat gegevens niet mogen verwerkt (en ook niet bekend mogen worden gemaakt) voor onverenigbare doeleinden binnen het beginsel van verdere doorgifte (alsmede het opt-outbeginsel).

Noodzaak van aanvullende verplichtingen voor privacyschildorganisaties die als verwerker (vertegenwoordiger) optreden en gegevens doorgeven naar een andere verwerker (vertegenwoordiger)

Het ontbreken van duidelijke voorschriften wanneer de privacyschildorganisatie als vertegenwoordiger optreedt (d.w.z. namens een EU-verwerkingsverantwoordelijke), duidt op een lacune en kan ertoe leiden dat de EU-verwerkingsverantwoordelijke de controle verliest. Een privacyschildorganisatie die als vertegenwoordiger van een EU-verwerkingsverantwoordelijke de gegevens ontvangt, moet de instructies van de EU-verwerkingsverantwoordelijke opvolgen. Dit moet in de beginselen duidelijk worden aangegeven om ervoor te zorgen dat niet-nakoming van deze instructies niet alleen schending van de overeenkomst betekent (bijlage II, punt III.10.a.ii), maar ook een schending van de privacyschildbeginselen inhoudt.

De mogelijkheid voor een schildorganisatie die als vertegenwoordiger optreedt om vervolgens gegevens door te geven aan een derde vertegenwoordiger moet transparant worden gemaakt voor de verwerkingsverantwoordelijke en onderworpen zijn aan voorafgaande goedkeuring door de verwerkingsverantwoordelijke. Daarom moet duidelijk worden aangegeven dat de overeenkomst die is getekend door de vertegenwoordiger met de EU-

verwerkingsverantwoordelijke (in FAQ 10 het "artikel 17-contract" genoemd) bepaalt of verdere doorgifte is toegestaan[22].

De huidige voorwaarden die van toepassing zijn op de verdere doorgifte naar een vertegenwoordiger zijn gebaseerd op de veronderstelling dat de privacyschildorganisatie optreedt als verwerkingsverantwoordelijke en daarom zelf kan beslissen over de mogelijke inmenging van een derde vertegenwoordiger. Dit moet echter niet mogelijk zijn als de privacyschildorganisatie optreedt als vertegenwoordiger. Anders verliest de EU-verwerkingsverantwoordelijke zijn controlecapaciteit.

De relevante privacybepalingen van de met de derde vertegenwoordiger gesloten overeenkomst moeten aan de verwerkingsverantwoordelijke beschikbaar worden gesteld en moeten ook ten minste hetzelfde beschermingsniveau bieden als de overeenkomst met de verwerkingsverantwoordelijke.

2.2.4 Gegevensintegriteit en doelbinding

a) Evenredigheid

Op een minder belangrijk punt verwijst WP29 naar haar brief aan vicevoorzitter Reding waarin zij vermeldt dat het mogelijk is dat een verwerking van persoonsgegevens, zelfs met strikte inachtneming van het kennisgevingsbeginsel en het keuzebeginsel, niet evenredig is als het gaat om de belangen, rechten en vrijheden van de betrokkene of de maatschappij. Het beginsel van evenredigheid of redelijkheid moet in elk stadium van de verwerking worden nageleefd en in aanvulling op de beginselen van kennisgeving en keuze van toepassing zijn[23].

In het privacyschildbesluit (bijlage II, punt II.5.a) wordt bepaald dat de informatie moet worden beperkt tot wat relevant is voor de verwerking. WP29 zou er de voorkeur aan geven als deze formulering in het definitieve adequaatheidsbesluit wordt gewijzigd, omdat enkel het feit dat de gegevens relevant zullen zijn voor de verwerking niet voldoende is om de verwerking evenredig te maken. Teneinde te voldoen aan het evenredigheidsbeginsel moet de verwerking worden beperkt tot gegevens die nodig zijn voor de betreffende verwerking.

b) Nauwkeurigheid

Het beginsel van de integriteit van gegevens en doelbinding (bijlage II, punt II.5) geeft ook aan: "Voor zover dit voor deze doeleinden noodzakelijk is, moet een organisatie redelijke stappen ondernemen om ervoor te zorgen dat de gegevens betrouwbaar zijn voor het beoogde gebruik en dat ze correct, volledig en actueel zijn". WP29 merkt op dat dit precies dezelfde formulering is als gebruikt in de veiligehavenregeling. WP29 betwijfelt of de formulering "voor zover dit voor deze doeleinden noodzakelijk is" moet worden opgenomen, omdat de nauwkeurigheid van de gegevens in haar optiek niet afhankelijk moet zijn van het doel van de

[22] Zie punt 4, onder "Onward Transfer", van de brief van WP29 aan vicevoorzitter Reding van 10 april 2014.
[23] Zie de brief van WP29 aan vicevoorzitter Reding van 10 april 2014.

verwerking. WP29 zou er de voorkeur aan geven als dit verband niet wordt gelegd in het definitieve adequaatheidsbesluit.

c) Doelbinding

Wanneer persoonsgegevens worden doorgegeven aan een organisatie in de VS door een in de EU gevestigde verwerkingsverantwoordelijke, moet de gegevensexporteur de Amerikaanse organisatie informeren over de doelen waarvoor de gegevens oorspronkelijk werden verzameld. Het is heel belangrijk om vast te stellen of een wijziging van het doel optreedt na de doorgifte, daarmee de beginselen van kennisgeving en keuze oproepend, en of deze wijziging zou bijdragen aan de verdeling van risico en aansprakelijkheid.

Het beginsel van integriteit van gegevens en doelbinding (bijlage II, punt II.5) geeft aan dat een organisatie geen persoonlijke informatie mag verwerken op een wijze die onverenigbaar is met de doeleinden waarvoor zij is verzameld of vervolgens goedgekeurd door de persoon. Het keuzebeginsel (bijlage II, punt II.2) voorziet echter in een opt-in voor het "gebruik" van gevoelige informatie (d.w.z. persoonlijke informatie over de gezondheid, raciale of etnische afkomst, politieke opvattingen, godsdienstige of filosofische overtuigingen, lidmaatschap van een vakbond of informatie over het seksleven van de betrokkene, alsmede gegevens met betrekking tot een strafblad) voor doelen die materieel verschillen van de doelen waarvoor de gegevens oorspronkelijk werden verzameld of vervolgens goedgekeurd door de persoon. Deze opt-in is niet vereist in de situaties die worden vermeld in aanvullend beginsel 1.a (bijlage II, punt III.1.a). Met betrekking tot niet-gevoelige persoonlijke informatie is voorzien in een opt-outregeling.

WP29 merkt op dat de werkingssfeer van het beginsel van doelbinding anders is onder de beginselen van kennisgeving, keuzemogelijkheid en gegevensintegriteit en doelbinding. In feite worden de termen "onverenigbaar doel" en "materieel verschillend doel" in dezelfde tekst gebruikt zonder een duidelijke definitie van beide begrippen[24].

WP29 maakt zich ernstig zorgen over de mogelijkheid dat een dergelijke inconsistentie het zeer moeilijk zal maken om het beginsel van gegevensintegriteit en doelbinding (bijlage II, punt II.5) in overeenstemming te brengen met het keuzebeginsel (bijlage II, punt II.2), omdat het ene aangeeft dat de gegevens niet verwerkt mogen worden op een wijze die onverenigbaar is met de doelen waarvoor ze werden verzameld, terwijl het andere voorziet in een opt-outmechanisme in het geval dat de gegevens worden verwerkt voor een doel dat wezenlijk anders is dan het oorspronkelijke doel.

Daarom kan het keuzebeginsel worden uitgelegd als het toestaan van een verder onverenigbare verwerking[25]. Volgens WP29 moet duidelijk worden gemaakt dat een

[24] WP29 merkte op dat ook een aantal andere uitdrukkingen wordt gebruikt: "gebruik dat afwijkt van" (bijlage II, punt III.14.b.ii), "gebruik voor andere doeleinden" (bijlage II, punt III.9.b.i), "gebruik voor een ander doel dan waarvoor deze oorspronkelijk is verzameld" (bijlage II, punt II.1.b). Deze onduidelijkheid kan leiden tot het ontbreken van voldoende garanties met betrekking tot het doelbindingsbeginsel.

[25] Zie ook de opmerking bij het keuzebeginsel. WP29 is van mening dat het feit dat de voorschriften inzake verdere doorgifte (bijlage II, punt II.3) alleen verwijzen naar het keuzebeginsel en niet naar het beginsel van doelbinding, het risico van een dergelijke uitleg doet toenemen.

organisatie niet bevoegd is om gegevens te verwerken voor een materieel verschillend doel, wanneer dit doel onverenigbaar is volgens het doelbindingsbeginsel. Met andere woorden, het moet duidelijk zijn dat het keuzebeginsel geen vrijstelling van doelbinding inhoudt.

Wanneer de verdere verwerking als verenigbaar kan worden beschouwd, moeten de beginselen van kennisgeving en keuze hoe dan ook van toepassing zijn.

2.2.5 Uitzonderingen voor journalistieke doeleinden

De uitzonderingen voor journalistieke doeleinden op de verwerking van persoonsgegevens worden besproken in aanvullend beginsel 2 (bijlage II, punt III.2). Bekend is dat deze bepalingen de wettelijke bescherming van de vrijheid van meningsuiting in de VS weergeven. Daarom geven de documenten van het privacyschild aan: "persoonlijke informatie uit eerder gepubliceerd materiaal dat via media-archieven wordt verspreid, is niet onderworpen aan de eisen van de privacyschildbeginselen" (bijlage II, punt III.2.b). Deze uitzondering lijkt elke verdere verwerking door een verwerkingsverantwoordelijke of verwerker te omvatten, met andere woorden, niet beperkt te worden tot verdere verwerking voor journalistieke doeleinden. Zoals al is aangegeven in de brief aan vicevoorzitter Reding van 10 april 2014, zou WP29 er de voorkeur aan geven om een beperktere aanpak te zien van uitzonderingen voor journalistieke doeleinden, die meer in lijn is met het in de EU toegepaste beginsel, alsmede het recht om te worden vergeten, naar aanleiding van het arrest-Google Spain[26].

2.2.5 Recht van toegang/inzage, rectificatie en wissing voor betrokkenen

Volgens het privacyschild hebben personen het recht om *bevestiging* te verkrijgen of hun gegevens worden verwerkt door een organisatie en om van dergelijke gegevens *in kennis te worden gesteld* (bijlage II, punt III.8.a.i). Echter, de verplichting voor organisaties om vragen van personen te beantwoorden over de doeleinden van de verwerking, over de categorieën persoonsgegevens waarop de verwerking betrekking heeft en over de ontvangers of de categorieën ontvangers aan wie de gegevens worden verstrekt, is tamelijk zwak. WP29 is van mening dat de aan betrokkene te verstrekken gegevens moeten worden vermeld in de lopende tekst zelf, en niet alleen maar in een voetnoot, en moeten worden opgesteld als een duidelijke verplichting (gekoppeld aan bijlage II, punt III.8.a.i.1).

Overeenkomstig aanvullend beginsel 8 "[behoeft] een organisatie alleen toegang tot door haar opgeslagen informatie te verlenen" (bijlage II, punt III.8.d.ii). Dit voorschrift moet niet restrictief worden uitgelegd, in de zin dat in principe toegang moet worden verschaft tot gegevens die op enige manier door een organisatie worden verwerkt, en niet alleen worden opgeslagen. Daarom is het belangrijk om, met het doel van de doeltreffendheid van het recht van toegang/inzage, duidelijk te maken dat "opslaan" "verwerken" betekent volgens de definitie in bijlage II, punt I.8.b. De toepassing van dit voorschrift moet tijdens de gezamenlijke toetsing van het privacyschild nauwkeurig worden onderzocht.

[26] Zaak C-131/12 – Google Spain / Agencia Española de Protección de Datos en Mario Costeja González, 13 mei 2014.

Zorgen blijven bestaan met betrekking tot de lijst van uitzonderingen in bijlage II, punt III.8.e, onder i), die vergelijkbaar is met de lijst in FAQ 8 van de veiligehavenregeling en ernaar neigt de belangen van de organisaties zwaarder te laten wegen. Zo zal geen toegang tot (inzage in) de eigen persoonsgegevens worden verleend als dat zou leiden tot: "schending van beroepsrechten of -plichten" (bijlage II, punt III.8.e.3), "conflict met veiligheidsonderzoeken of klachtenprocedures waarbij werknemers zijn betrokken of in verband met personeelsbeleid en bedrijfsherstructurering" (bijlage II, punt III.8.e.4), of "aantasting van de geheimhouding die noodzakelijk is voor toezichthoudende of regulerende taken in verband met een gezond beheer of bij toekomstige of lopende onderhandelingen in verband met de organisatie" (bijlage II, punt III.8.e.5). Deze redenen moeten worden gelezen in samenhang met de algemene uitzonderingspositie van vertrouwelijke commerciële informatie, die is opgenomen in bijlage II, punt III.8.c. Daarom zal iemand in de hierboven opgesomde situaties nooit toegang krijgen tot zijn of haar gegevens en zal er niet worden gezocht naar een evenwicht tussen de rechten en belangen van de persoon en die van de organisatie om tot een oplossing voor het verzoek om toegang te komen.

WP29 wijst erop dat het recht van personen op inzage in hun eigen gegevens wordt gewaarborgd in artikel 8, lid 2, van het Handvest van de grondrechten. Hoewel dit geen absoluut recht is, is het fundamenteel voor het recht op de bescherming van persoonsgegevens omdat het de uitoefening van de andere rechten van de betrokkene vergemakkelijkt, zoals rectificatie en wissing.

Wat het recht op rectificatie en wissing betreft, is WP29 verheugd over een aanzienlijke verbetering die de privacyschildbeginselen bieden ten opzichte van de veiligehavenbeginselen, namelijk dat deze rechten niet alleen gelden in situaties wanneer gegevens onnauwkeurig zijn, maar ook wanneer gegevens in strijd met de beginselen zijn verwerkt (bijlage II, punt II.6).

2.2.6 Verhaal, handhaving en aansprakelijkheid (verhaalmechanismen)

a) Doeltreffende uitoefening van de verhaalrechten van natuurlijke personen in de EU

WP29 erkent de verbintenissen van de autoriteiten van de VS met betrekking tot de verschillende lagen van het verhaalmechanisme. Gezien de complexiteit en het gebrek aan duidelijkheid van de algehele opzet van het mechanisme vreest WP29 echter dat de doeltreffende uitoefening van de rechten van betrokkenen in de praktijk ondermijnd kan worden. WP29 wijst erop dat de kwaliteit van het verhaalmechanisme moet prevaleren boven de kwantiteit van mechanismen die beschikbaar zijn voor natuurlijke personen in de EU. Zij is ook bezorgd dat voor de meeste, zo niet alle, verhaalmechanismen wordt voorzien in een procedure in de VS, waardoor het toezicht op de procedure door de gegevensbeschermingsautoriteiten van de EU wordt bemoeilijkt.

Het verhaalmechanisme waarin het privacyschild voorziet, concentreert zich namelijk in de eerste plaats op de mogelijkheid voor de betrokkene om zijn rechten te handhaven en zich bij niet-naleving van de privacyschildbeginselen rechtstreeks te wenden tot de zelf-

gecertificeerde onderneming in de VS[27]. Bovendien moeten organisaties een onafhankelijk orgaan voor geschillenbeslechting aanwijzen om individuele klachten te onderzoeken en op te lossen. WP29 is verheugd over het feit dat dit zal worden geregeld zonder kosten voor natuurlijke personen.

Als alternatief kunnen klachten rechtstreeks worden ingediend bij de Federal Trade Commission (FTC), ook als deze niet verplicht is om die te behandelen. De gegevensbeschermingsautoriteit kan een klacht ook doorverwijzen; het DoC heeft beloofd om deze te toetsen en om zich in te spannen de oplossing van klachten (bijlage I) te vergemakkelijken. Daaraan zal door de FTC prioriteit worden gegeven (bijlage II, punt III.7.e). De prioriteit die de FTC aan klachten geeft, biedt de betrokkene echter geen zekerheid dat zijn klachten zullen worden behandeld.

In laatste instantie hebben burgers de mogelijkheid om een beroep te doen op bindende arbitrage. Het arbitragepanel zal worden gevestigd in de VS en zal worden onderworpen aan toetsing door de Amerikaanse rechter.

Het privacyschild biedt de organisatie ook de mogelijkheid om samenwerking met de gegevensbeschermingsautoriteiten van de EU te verkiezen (bijlage II, punt III.5.a). Dit is zelfs verplicht voor personeelsgegevens die zijn verzameld in de context van een arbeidsverhouding (bijlage II, punt III.9.d.ii). In een dergelijk scenario zal alternatieve geschillenbeslechting (ADR) niet van toepassing zijn (bijlage II, punt III.5.a). Het privacyschild stelt niet duidelijk vast hoe de samenwerking met EU-gegevensbeschermingsautoriteiten in de praktijk georganiseerd zal worden. In het bijzonder is het onduidelijk of het panel alle zaken zal behandelen of dat elke afzonderlijke zaak door een ander panel zal worden behandeld.

WP29 is van mening dat het adequaatheidsbesluit uitvoeriger moet zijn als het gaat om de bevoegdheid van de gegevensbeschermingsautoriteiten om klachten te behandelen. Dit is kennelijk afhankelijk van de kwalificatie van de organisatie, maar het is onduidelijk op welke manier.

Wanneer de organisatie namens een EU-verwerkingsverantwoordelijke optreedt als een vertegenwoordiger, zullen personen in elk geval de mogelijkheid hebben om een klacht in te dienen tegen een bevoegde gegevensbeschermingsautoriteit in de EU. De situatie zal vergelijkbaar zijn voor de verwerking van personeelsgegevens en andere commerciële gegevens.

Wanneer de privacyschildorganisatie optreedt als verwerkingsverantwoordelijke, zal de bevoegdheid van een gegevensbeschermingsautoriteit om de klacht te behandelen beperkt zijn tot verwerking die onderworpen is aan het EU-recht: wanneer de verwerking gebeurt onder verantwoordelijkheid van een EU-verwerkingsverantwoordelijke – inclusief gezamenlijke controle met een Amerikaanse organisatie – of wanneer de privacyschildorganisatie rechtstreeks onder het EU-recht zou vallen, bijvoorbeeld doordat zij gebruikmaakt van

[27] Europese Commissie, ontwerp-adequaatheidsbesluit, punt 30.

apparatuur in de EU. Voor gegevensverwerking die alleen onder Amerikaans recht wordt uitgevoerd, zullen echter uitsluitend de mechanismen van het privacyschild van toepassing zijn. Teneinde taalbarrières en een gebrek aan kennis van het rechtsstelsel te overwinnen, kan het nuttig zijn als de EU-gegevensbeschermingsautoriteiten mogen optreden als tussenpersoon voor de klacht van de persoon of hem/haar bij mogen staan in ADR-zaken met organisaties in de VS of bij hun contacten met de autoriteiten van de VS, als de gegevensbeschermingsautoriteit dat gepast acht.

WP29 benadrukt dat het in het privacyschild uiteengezette mechanisme de eerdere aanbeveling niet volgt, die inhield dat natuurlijke personen in de EU schadeklachten kunnen indienen in de Europese Unie en een klacht mogen indienen bij een bevoegde nationale rechtbank in de EU[28]. Het zou op prijs worden gesteld als privacyschildorganisaties deze mogelijkheid in hun privacybeleid zouden opnemen.

Teneinde effectiviteit te waarborgen, adviseert WP29 dat het systeem er bij voorkeur voor zorgt dat EU-gegevensbeschermingsautoriteiten de betrokkene kunnen vertegenwoordigen en namens hem/haar of als tussenpersoon kunnen optreden. Anderzijds moet het systeem specifieke rechtsbevoegdheidsbepalingen omvatten die betrokkenen het recht geven om hun rechten in Europa uit te oefenen.

b) Arbitrage

De definitieve arbitrageprocedures zijn nog niet afgerond, hetgeen de beoordeling van WP29 bemoeilijkt. Als blijkt dat de arbitrageregeling volgens Amerikaans recht zal verlopen en de enige proceduretaal het Engels zal zijn, willen EU-gegevensbeschermingsautoriteiten het recht hebben om personen bij te staan in het proces.

Bovendien is de arbitrageprocedure opgezet vanwege het feit dat er geen garantie is dat een klacht zal worden behandeld, aangezien de FTC niet verplicht is om elke klacht te behandelen. WP29 merkt op dat als een natuurlijke persoon in de EU het nodig vindt om zich te laten bijstaan door een advocaat, die persoon zelf het honorarium van zijn advocaat moet betalen, hetgeen personen ervan zal weerhouden om hun klacht aan de arbitrageprocedure voor te leggen.

c) Toezicht, handhaving en effectiviteit van verhaalmechanismen

<u>Voorwaarden om tot het schild toe te treden</u>

Volgens het HvJEU “hangt de betrouwbaarheid van een [systeem van zelfcertificering] […] hoofdzakelijk af van de invoering van doeltreffende detectie- en controlemechanismen waarmee in de praktijk eventuele schendingen van de regels ter bescherming van de grondrechten […] kunnen worden vastgesteld”[29].

[28] Zie de brief van WP29 aan vicevoorzitter Reding, 10 april 2014.
[29] HvJEU, Schrems, punt 81.

WP29 merkt op dat de rol van het DoC bij het certificeringsproces in het privacyschild beperkt lijkt te worden tot enkel een controle op de volledigheid van documenten. Hoewel WP29 erkent dat zelfcertificering geen systematische voorafgaande controle impliceert van de uitvoering van het privacybeleid, moet het DoC zich er op zijn minst toe verbinden systematisch te zullen controleren dat het privacybeleid alle privacyschildbeginselen omvat. Deze verbintenis wordt genoemd in het ontwerp-adequaatheidsbesluit, maar kan niet duidelijk worden geïdentificeerd in de verklaring ("representation letter") van het DoC[30].

Een schending van de privacyschildbeginselen kan gedurende een lange tijd onopgemerkt blijven en pas ontdekt worden nadat ernstige en mogelijk onomkeerbare schade is toegebracht aan de grondrechten van de betrokkene. Deze aanpak kan dus inbreuk maken op het Europese voorzorgsbeginsel.

Transparantie door middel van de privacyschildlijst en register van organisaties die van de lijst zijn verwijderd

Er zijn aanzienlijke verbeteringen aangebracht met betrekking tot de transparantie ten aanzien van de betrokkene. Naast alle Amerikaanse organisaties die bij het DoC een zelfcertificeringsverklaring hebben ingediend, zal de nieuwe privacyschildlijst ook een register omvatten van alle organisaties die van de privacyschildlijst zijn verwijderd, met inbegrip van de reden waarom een organisatie is verwijderd[31]. De privacyschildwebsite van het DoC zal zich bovendien duidelijker richten op het doelpubliek, zodat gemakkelijker kan worden geverifieerd wat voor informatie onder de zelfcertificering van een organisatie valt en wat het privacybeleid inhoudt dat op die informatie van toepassing is, en welke methode de organisatie gebruikt om haar naleving van de beginselen te controleren[32]. WP29 is verheugd over het feit dat nu duidelijk is dat het DoC zal controleren of bedrijven die een openbare website hebben, hun privacybeleid op deze website hebben gepubliceerd of, als ze geen openbare website hebben, waar het privacybeleid beschikbaar wordt gesteld voor het publiek[33]. De documenten geven ook meer informatie over de inhoud van het privacybeleid[34].

WP29 is van mening dat er een probleem kan optreden als een organisatie die al op de privacyschildlijst staat, vervolgens haar certificering uitbreidt naar andere categorieën gegevens. In dergelijke gevallen zal de lijst de verschillende perioden van toepasselijkheid van de beginselen op de verschillende categorieën gegevens niet weergeven. Dit schept een risico dat EU-burgers en bedrijven niet volledig kunnen vaststellen of een specifiek bestand inderdaad onderworpen is aan de privacyschildbeginselen, en zo ja, sinds wanneer. Om deze tekortkoming te vermijden, adviseert de werkgroep dat de registratie van een organisatie op

[30] Europese Commissie, ontwerp-adequaatheidsbesluit, punt 34.
[31] Bijlage I, blz. 5, en bijlage II, punt II.1; WP29 verwijst ook naar de vierde aanbeveling van de Commissie in de mededeling COM(2013) 847 alsmede naar de brief van WP29 aan vicevoorzitter Reding van 10 april 2014, in het bijzonder punt 5 onder "Transparency".
[32] Bijlage I, blz. 8; WP29 verwijst ook naar haar brief aan vicevoorzitter Reding, 10 april 2014, in het bijzonder punt 2 onder "Transparency".
[33] Bijlage I, blz. 3 en 4; WP29 verwijst ook naar de eerste aanbeveling van de Commissie in de mededeling COM(2103) 847 alsmede naar de brief van WP29 aan vicevoorzitter Reding, 10 april 2014, in het bijzonder punt 3 onder "Transparency".
[34] Bijlage I, blz. 5 en 6, en bijlage II, punt III.6.

de privacyschildlijst voor elke categorie persoonsgegevens afzonderlijk vermeldt sinds welke datum op die gegevens de zelfcertificering van toepassing is.

WP29 verwelkomt het feit dat het DoC een register met van de privacyschildlijst verwijderde organisaties zal bijhouden en dat deze registratie een verklaring zal omvatten die duidelijk maakt dat deze organisaties niet langer verzekerd zijn van de voordelen van het privacyschild, maar de beginselen moeten blijven toepassen op ontvangen persoonsgegevens omdat ze een gecertificeerde organisatie van het privacyschild zijn, zolang zij dergelijke gegevens bewaren (bijlage I, blz. 3). Aangezien sommige organisaties die van de privacyschildlijst zijn verwijderd, kunnen kiezen om de in het kader van het privacyschild ontvangen gegevens terug te sturen of te wissen, terwijl andere organisaties gegevens bewaren die ze in het kader van het schild hebben ontvangen, is het echter belangrijk om burgers in deze kwestie meer transparantie te verschaffen. Daarom moet het register van bedrijven dat door het DoC wordt bijgehouden, vermelden of de organisatie nog steeds persoonsgegevens bewaart onder het privacyschild, of dat ze deze gegevens heeft teruggestuurd of gewist. Als de organisatie deze gegevens nog steeds bewaart, moet de registratie uitdrukkelijk aangeven dat de organisatie de beginselen moet blijven toepassen op deze gegevens.

Bovendien moet in het door het DoC bewaarde register zijn opgenomen dat deze organisaties niet langer verzekerd zijn van de voordelen van het privacyschild voor nieuwe doorgiften, hetgeen inhoudt dat de organisatie niet langer persoonsgegevens van de EU onder de beginselen mag ontvangen.

Controleprocedures

Om te controleren of de zelfcertificering in de praktijk doeltreffend is, kunnen organisaties een zelfbeoordeling uitvoeren of aan een externe nalevingscontrole worden onderworpen. WP29 betreurt het dat het opleiden van werknemers uitsluitend is vereist als een organisatie kiest voor controle door middel van zelfbeoordeling (bijlage II, punt III.7.c). Bovendien lijkt het erop dat de noodzaak om te controleren of beleid zorgvuldig en allesomvattend is, duidelijk wordt bekendgemaakt, volledig wordt uitgevoerd en toegankelijk is, alleen bestaat als de organisatie kiest voor interne controle (zelfbeoordeling) en dat controle door middel van een extern mechanisme slechts beperkt is tot de naleving van het privacybeleid van de organisatie.

A posteriori

WP29 verwelkomt het feit dat de FTC en het DoC over onderzoeksbevoegdheden beschikken wanneer er sprake is van klachten. Bovendien merkt WP29 op dat het DoC de mogelijkheid zal hebben om ambtshalve controles uit te voeren, in het bijzonder door het versturen van vragenlijsten. WP29 wil er echter van verzekerd zijn dat een dergelijke aanpak voldoende is om te voldoen aan de eis van het HvJEU met betrekking tot doeltreffende detectie- en supervisiemechanismen in geval van overtreding. WP29 heeft nog steeds vragen over de exacte bevoegdheid van de Amerikaanse handhavingsautoriteiten om op de bedrijfsterreinen van organisaties met een zelfcertificering inspecties ter plaatse uit te voeren teneinde

overtredingen van het privacyschild te onderzoeken, over hoe het exequatur van een beslissing van een EU-autoriteit kan worden verkregen op Amerikaans grondgebied en of de sancties krachtens het privacyschild in de praktijk een afschrikkend effect hebben.

2.2.7 Verwerking van personeelsgegevens

Toepassingsgebied

Aanvullend beginsel 9 (bijlage II, punt III.9) is van toepassing op persoonlijke informatie over een (vroegere of huidige) werknemer verzameld in de context van de arbeidsverhouding. Volgens de formulering van het aanvullend beginsel 9.a.ii, zijn de privacyschildbeginselen alleen van toepassing wanneer "bestanden over individueel bepaalde of bepaalbare personen worden doorgegeven of toegankelijk worden gemaakt". De term "bestanden over individueel bepaalde personen" stemt niet overeen met de definitie van "persoonsgegevens" in bijlage I.8.a, die "gegevens over een geïdentificeerde of identificeerbare natuurlijke persoon" luidt, en komt daardoor niet overeen met de definitie in de richtlijn[35].

Aanvullend beginsel 9.a.ii geeft aan dat "statistische informatie die berust op geaggregeerde personeelsgegevens en geen persoonsgegevens bevat of het gebruik van geanonimiseerde gegevens, geen aanleiding [geeft] tot problemen in verband met de bescherming van de persoonlijke levenssfeer". Deze stelling spreekt een aantal adviezen van WP29 tegen. WP29 wil benadrukken dat geaggregeerde gegevens nog steeds opnieuw kunnen worden geïdentificeerd en daarom moeten worden beschouwd als persoonsgegevens[36].

Kennisgeving, keuzemogelijkheid en doelbinding

Aanvullend beginsel 9.b.i geeft een voorbeeld van de toepassing van het kennisgevingsbeginsel en het keuzebeginsel, waarbij personeelsgegevens worden gebruikt voor een ander doel. Het voorbeeld heeft betrekking op een Amerikaanse organisatie die "van plan is persoonlijke informatie die in het kader van een arbeidsverhouding is verzameld, te gebruiken voor doeleinden die niet met de arbeidsrelatie te maken hebben, zoals commerciële mededelingen". In dit scenario is de wijziging van het doel toegestaan op voorwaarde dat het kennisgevingsbeginsel en het keuzebeginsel in acht worden genomen. Volgens WP29 zal de verdere verwerking van personeelsgegevens voor directmarketingdoeleinden in de meeste gevallen moeten worden beschouwd als een onverenigbaar doel en daarom in strijd zijn met het beginsel van doelbinding (bijlage II, punt II.5.a). Bovendien is WP29 van mening dat het keuzebeginsel geen geschikte basis kan zijn voor de werknemer om "toestemming te geven" (opt-out) voor een wijziging van het doel, in de context van een dienstverband waarbij een dergelijke toestemming niet geheel vrijwillig zou kunnen zijn.

WP29 betwijfelt sterk of de belangrijkste focus van het privacyschild op het keuzebeginsel als voorwaarde om gegevens verder te gebruiken voor een ander doel, voldoet aan de privacyrichtlijnen van de OESO, omdat er niet voldoende garanties zijn om te voorkomen dat

[35] Zoals reeds is onderstreept, is de beperking tot bestanden die "doorgegeven of toegankelijk worden gemaakt" evenmin in overeenstemming met de definitie van "verwerking" (bijlage II, punt I.8.b).
[36] Zie advies 4/2007 over het begrip persoonsgegeven en advies 05/2014 over anonimiseringstechnieken.

dit opt-outmechanisme ook wordt gebruikt voor verdere onverenigbare verwerking. Aanvullend beginsel 9.b.iv voorziet in een ruime en uitdrukkelijke vrijstelling van het kennisgevingsbeginsel en het keuzebeginsel "voor zover en zolang het noodzakelijk is om te voorkomen dat afbreuk wordt gedaan aan de mogelijkheid van een organisatie om besluiten inzake bevorderingen of benoemingen of andere besluiten ten aanzien van de werknemers te nemen". Op de eerste plaats moet het gebruik van personeelsgegevens voor dergelijke doeleinden al uitdrukkelijk worden aangegeven bij het verzamelen van de gegevens. Bovendien is de formulering "andere besluiten ten aanzien van de werknemers" te vaag en te ruim. Dientengevolge zullen personeelsgegevens, wanneer deze wordt verwerkt in de context van de arbeidsverhouding, volledig worden vrijgesteld van het kennisgevingsbeginsel en het keuzebeginsel. De term is zo ruim dat het niet mogelijk is om te beoordelen of het toekomstige gebruik verenigbaar is met het oorspronkelijke doel. WP29 beveelt aan dat deze uitzondering wordt geschrapt.

Recht van toegang/inzage

Aanvullend beginsel 9.e.i voorziet ook in een vrijstelling voor de toepassing van het beginsel van toegang of voor het sluiten van een overeenkomst met een derde verwerkingsverantwoordelijke inzake personeelsgegevens, indien deze betrekking hebben op incidentele werkgerelateerde handelingen, zoals het boeken van een vlucht of hotelkamer of het sluiten van een verzekering, doorgifte van persoonsgegevens van een klein aantal werknemers, mits wordt voldaan aan het kennisgevingsbeginsel en het keuzebeginsel. WP29 ziet geen redelijke rechtvaardiging voor een dergelijke vrijstelling en adviseert om deze paragraaf te schrappen.

2.2.8 Farmaceutische en medische producten

Toepassingsgebied

Volgens het privacyschild gelden doorgiften van met een unieke code versleutelde gegevens van de Europese Unie naar de VS in de context van farmaceutische en medische producten niet als doorgiften die onderworpen zijn aan het privacyschild (bijlage II, punt III.14.g.i). De doorgifte van met een unieke code versleutelde gegevens geniet echter bescherming krachtens het Europese gegevensbeschermingsrecht. Dit betekent dat het privacyschild in de praktijk dergelijke doorgiften niet kan ondersteunen. WP29 vraagt de Europese Commissie met klem om uitdrukkelijk te bepalen dat het ontwerp-adequaatheidsbesluit de doorgifte van met een unieke code versleutelde gegevens om farmaceutische of medische redenen niet zal ondersteunen; dientengevolge moeten zulke doorgiften worden gedekt door andere waarborgen, zoals modelcontractbepalingen of bindende bedrijfsvoorschriften. WP29 stelt voor dat dit kan worden toegelicht in het definitieve adequaatheidsbesluit.

Doorgiften met het oog op regelgeving en toezicht (bijlage II, punt III.14.d)

WP29 maakt zich zorgen dat op grond van deze bepalingen persoonsgegevens in de medische context die overwegend gevoelig van aard zijn, kunnen worden doorgegeven aan

regelgevende instanties in de VS. Aangezien het privacyschild is ontworpen voor doorgiften van gegevens tussen particuliere entiteiten, lijkt het erop dat een openbaar orgaan zoals een regelgevende instantie in de VS niet in aanmerking komt voor zelfcertificering onder het privacyschild, wat de vraag doet rijzen of dergelijke doorgiften passende gegevensbescherming genieten. Als dergelijke doorgiften moeten worden beheerd voor regelgevingsdoeleinden, moeten passende maatregelen worden genomen om de voortdurende bescherming van de grondrechten van betrokkenen in de EU te waarborgen. WP29 onderstreept dat het ontwerp-adequaatheidsbesluit geen uitspraken doet op dit punt. Daarom is er volgens WP29 geen enkele garantie dat gevoelige gegevens van betrokkenen in de EU in deze context passende bescherming zullen genieten.

Bovendien merkt WP29 op dat zij niet begrijpt waarom het doel "verkoopactiviteiten" wordt vermeld als voorbeeld van verwerking voor toekomstig wetenschappelijk onderzoek. Ook de reden om verdere doorgiften naar bedrijfslocaties en andere onderzoekers (bijlage II, punt III.14.d) te plaatsen onder het kopje "doorgiften met het oog op regelgeving en toezicht" is niet duidelijk. Deze kwesties moeten in het definitieve adequaatheidsbesluit worden opgehelderd.

Toezicht op productveiligheid en -efficiëntie (inclusief rapportage aan overheidsinstanties) en het volgen van patiënten die bepaalde geneesmiddelen of medische hulpmiddelen gebruiken

Het privacyschild voorziet in een vrijstelling van de beginselen van kennisgeving, keuze, verdere doorgifte en toegang/inzage, voor zover het volgen van het beginsel de naleving van wettelijke eisen in de weg zou staan. Het ontwerp-adequaatheidsbesluit doet geen uitspraak over situaties waarin de privacybeginselen de naleving van wettelijke vereisten in de weg staan. Hoewel WP29 kan begrijpen dat onderzoek door de overheid beperkingen van het kennisgevingsbeginsel en het recht van toegang/inzage kan rechtvaardigen ter bescherming van het onderzoek, ziet WP29 geen redenen die dergelijke ruime vrijstellingen kunnen rechtvaardigen wanneer gegevens worden verwerkt door een organisatie of een derde partij in de particuliere sector. Als bijvoorbeeld de behandelingen van patiënten steeds meer worden geïndividualiseerd, is een dergelijke ruime vrijstelling van de privacybeginselen bij het volgen van patiënten die bepaalde geneesmiddelen of medische hulpmiddelen gebruiken onaanvaardbaar, aangezien dit type zorg algemeen zal worden. Dit geldt ook wanneer gegevens worden gebruikt door farmaceutische bedrijven voor toezicht op productveiligheid en -efficiëntie (test of verkoop van nieuwe geneesmiddelen).

2.2.9 Openbaar beschikbare informatie

De uitzondering op het recht van toegang in het geval van openbaar beschikbare informatie en informatie uit openbare bestanden (bijlage II, punt III.15.d en e) doet bezorgdheid rijzen voor zover dat een persoon, bij het uitoefenen van zijn/haar recht van toegang, wil weten of een specifieke verwerkingsverantwoordelijke gegevens over hem/haar verwerkt, en ook wil weten welke gegevens worden verwerkt, teneinde de verwerking van zijn/haar gegevens te kunnen controleren. WP29 heeft herhaaldelijk aangegeven dat betrokkenen volgens het EU-recht altijd recht van toegang tot hun gegevens hebben en waar nodig rectificatie of wissing kunnen

eisen als de gegevens niet rechtmatig zijn verwerkt of als ze onvolledig of onnauwkeurig zijn, ongeacht of de persoonsgegevens al dan niet zijn gepubliceerd[37]. Als het verzoek om toegang van een persoon wordt geweigerd op grond van het feit dat de gegevens zijn verkregen uit openbaar beschikbare bronnen of openbare bestanden, zou de persoon niet de mogelijkheid hebben om de nauwkeurigheid van de gegevens te controleren en om te controleren of de gegevens rechtmatig openbaar zijn gemaakt.

Het privacyschild stelt informatie uit openbare bestanden en openbaar beschikbare informatie echter vrij van de beginselen van kennisgeving, keuze, toegang en aansprakelijkheid voor verdere doorgifte (bijlage II, punt II.15.b). Deze uitzonderingen lijken te ruim in vergelijking met de richtlijn en doen zorgen rijzen omdat ze onder andere afbreuk doen aan de mogelijkheden van personen om de nauwkeurigheid van hun gegevens te controleren en verspreiding van hun gegevens te beperken.

2.3 Conclusies

WP29 erkent dat de Amerikaanse autoriteiten en de Europese Commissie hebben gezorgd voor aanzienlijke verbeteringen van de commerciële aspecten voor doorgifte van gegevens tussen de twee continenten. Rekening houdend met de bovengenoemde analyse is WP29 echter van mening dat het commerciële deel van het privacyschild op veel punten verdere opheldering vereist. Het gebrek aan een expliciet beginsel inzake gegevensbewaring strekt bijvoorbeeld tot bezorgdheid. WP29 maakt zich ernstige zorgen over de vraag of het privacyschild een beschermingsniveau kan garanderen dat in wezen overeenstemt met het beschermingsniveau in de EU.

Het adequaatheidsbesluit moet het beginsel van doelbinding en het beginsel van keuze verder toelichten. Het risico van lacunes met betrekking tot verschillende beginselen blijft bestaan, met name wat verdere doorgifte, het mechanisme voor de behandeling van klachten en het verwerken van personeels- of farmaceutische gegevens betreft. Bovendien moet verder worden uitgewerkt hoe de privacyschildbeginselen moeten worden toegepast op gegevensverwerkers (vertegenwoordigers) en moet specifiek aandacht worden besteed aan een duidelijke en ondubbelzinnige toepassing van terminologie.

3. BEOORDELING VAN DE NATIONALE VEILIGHEIDSWAARBORGEN VAN HET ONTWERP-ADEQUAATHEIDSBESLUIT

3.1 Waarborgen en beperkingen die van toepassing zijn op de nationale veiligheidsautoriteiten van de Verenigde Staten

Inmenging in de grondrechten inzake het privéleven en gegevensbescherming kan aanvaardbaar zijn, mits deze inmenging gerechtvaardigd is in een democratische maatschappij. Dit betekent dat de privacybeginselen niet absoluut zijn en dat afwijkingen mogelijk zijn, maar alleen als wordt voldaan aan de toepasselijke (essentiële) waarborgen. In overeenstemming met het doel om de privacybescherming te verbeteren, moeten organisaties

[37] Zie WP20, blz. 4

er bovendien naar streven om deze beginselen volledig en op transparante wijze uit te voeren, door ook in hun privacybeleid te vermelden in welke gevallen uitzonderingen op de beginselen als toegestaan door het Amerikaanse rechtskader, regelmatig van toepassing zullen zijn. Om dezelfde reden wordt, wanneer de optie is toegestaan krachtens de beginselen en/of de Amerikaanse wet, van organisaties verwacht dat zij waar mogelijk kiezen voor de hogere mate van bescherming.

In bijlage II, punt I.5 wordt aangegeven dat "De onderschrijving van deze Beginselen kan worden beperkt: a) voor zover nodig om te voldoen aan vereisten inzake nationale veiligheid, het algemeen belang of rechtshandhaving; b) op grond van de wet, overheidsreglementering of jurisprudentie die tegenstrijdige verplichtingen of uitdrukkelijke bevoegdheden creëert, op voorwaarde dat een organisatie bij het uitoefenen van een dergelijke bevoegdheid kan aantonen dat haar niet-naleving van de Beginselen niet verder gaat dan nodig is om te voldoen aan de dwingende legitieme belangen die door een dergelijke bevoegdheid worden bevorderd; of c) indien met de richtlijn of de wetgeving van de lidstaat wordt beoogd uitzonderingen of afwijkingen toe te staan, mits deze uitzonderingen of afwijkingen in vergelijkbare situaties worden toegepast."

De vraag is of de in bijlage II genoemde afwijkingen gerechtvaardigd zijn in een democratische maatschappij. Volgens het ontwerp-adequaatheidsbesluit van het privacyschild heeft de Commissie geconcludeerd "dat er in de Verenigde Staten regelgeving bestaat die bedoeld is om ingrepen ten behoeve van de nationale veiligheid in de grondrechten van de personen van wie persoonsgegevens uit de Unie naar de Verenigde Staten worden doorgegeven in het kader van het EU-VS-privacyschild, te beperken tot hetgeen strikt noodzakelijk is om het betrokken legitieme doel te bereiken."[38]

Aan de hand van het kader zoals uiteengezet in deel 1.2 van dit advies en rekening houdend met de vertegenwoordigingen van de Amerikaanse autoriteiten en de bevindingen van de Commissie, heeft WP29 het huidige rechtskader van de Verenigde Staten en de praktijken van Amerikaanse inlichtingendiensten geanalyseerd evenals de voorwaarden waaronder zij inmenging in de grondrechten inzake het privéleven en gegevensbescherming, zoals beschermd binnen het Europese rechtskader, toestaan. Deze beoordeling is gebaseerd op de analyse van de presidentiële beleidsrichtlijn 28 (PPD-28), uitvoeringsbevel 12333 (EO12333) en op de diverse rechtsgrondslagen zoals vastgesteld door de Foreign Intelligence Act (FISA - sectie 104, sectie 402, sectie 215, sectie 501 en sectie 702). WP29 heeft zich gebaseerd op bijlage VI van het privacyschild, die een brief van het bureau van de directeur van het nationale inlichtingenwerk (ODNI) bevat met betrekking tot waarborgen en beperkingen die van toepassing zijn op Amerikaanse nationale veiligheidsautoriteiten, evenals een samenvatting van de informatie die aan de Europese Commissie is verstrekt over de activiteiten van de Verenigde Staten op het gebied van het verzamelen van inlichtingen uit berichtenverkeer.

[38] Ontwerpbesluit van de Commissie overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de gepastheid van de door het EU-VS-privacyschild geboden bescherming, §75.

3.2 Waarborg A - Verwerking moet plaatsvinden in overeenstemming met het recht en op basis van duidelijke, nauwkeurige en toegankelijke voorschriften

Volgens het Europees recht moet inmenging in overeenstemming zijn met de regelgeving, vastgesteld beleid en vaste procedures en voldoende duidelijk en toegankelijk zijn (binnen de marge van aan individuele landen verleende beoordelingsvrijheid), zodat burgers duidelijk kunnen weten in welke omstandigheden en onder welke voorwaarden openbare organen hun toevlucht mogen nemen tot toezichtsmaatregelen[39].

WP29 merkt op dat activiteiten op het gebied van inlichtingen uit berichtenverkeer plaatsvinden op basis van een toegankelijk rechtskader. Alle wetten genoemd in bijlage VI (PPD-28, FISA, USA FREEDOM ACT, FOIA) zijn online beschikbaar voor het grote publiek (in en buiten de Verenigde Staten). Bijlage VI geeft een samenvatting van het toepasselijke rechtskader, de beperkingen wat het verzamelen betreft, de beperkingen wat opslag en verspreiding betreft, naleving en toezicht, transparantie en verhaal. Het Amerikaanse rechtsstelsel voor inlichtingenactiviteiten bestaat uit een aantal verschillende documenten, waaronder verslagen van afzonderlijke instanties, beleidsmaatregelen en procedures, die geanalyseerd moeten worden om meer inzicht te krijgen in de wijze waarop activiteiten worden uitgevoerd, zowel in theorie als in de praktijk. In dat opzicht heeft WP29 zich geconcentreerd op een beperkt aantal punten die zij zeer belangrijk acht.

3.2.1 Uitvoeringsbevel 12333 en presidentiële beleidsrichtlijn 28

De werkingssfeer van EO12333 is ruim: in principe kan iedere verzameling van buitenlandse inlichtingen plaatsvinden naar goeddunken van de Amerikaanse president, op basis van het bevel. Er is echter aangevoerd dat, sinds de introductie van FISA, EO12333 alleen kan worden gebruikt voor het verzamelen van gegevens buiten het Amerikaanse grondgebied. WP29 merkt op dat EO12333 niet veel gegevens verschaft over zijn geografische werkingssfeer, de mate waarin gegevens kunnen worden verzameld, bewaard of verder verspreid, of over de aard van strafbare feiten die aanleiding kunnen geven tot toezicht en het soort informatie dat kan worden verzameld of gebruikt.

Zoals WP29 het begrijpt, bestaat het belangrijkste doel van de presidentiële beleidsrichtlijn 28 (PPD-28) erin de beperkingen voor het verzamelen en verwerken van persoonsgegevens vast te leggen voor alle toezichtsprogramma's en ongeacht de bron van de gegevens.

[39] EHRM Zakharov §247 "Het Hof heeft eerder uitgelegd dat de eis van "voorzienbaarheid" van de wet niet zo ver gaat dat staten worden gedwongen juridische bepalingen vast te stellen die in detail elk gedrag vermelden dat aanleiding kan geven tot een besluit om een persoon te onderwerpen aan geheim toezicht om redenen van nationale veiligheid. Door de aard van de dingen kunnen bedreigingen voor de nationale veiligheid zeer uiteenlopend en niet te voorspellen of moeilijk vooraf te definiëren zijn (zie Kennedy, hierboven geciteerd, § 159). Tegelijkertijd heeft het Hof ook benadrukt dat in aangelegenheden die een invloed hebben op de grondrechten, het strijdig zou zijn met de rechtsstaat, een van de grondbeginselen van een democratische samenleving vastgelegd in het verdrag, als de voor uitvoering bevoegde op het gebied van nationale veiligheid beoordelingsvrijheid wordt verleend in termen van ongebreidelde bevoegdheid. Daarom moet de wet voldoende duidelijk de reikwijdte van de aan de bevoegde autoriteiten verleende beoordelingsvrijheid aangeven, evenals de manier waarop die wordt uitgeoefend, rekening houdend met het legitieme doel van de maatregel in kwestie, teneinde de burger passende bescherming te bieden tegen arbitraire inmenging."

PPD-28 is een richtlijn van de president van de Verenigde Staten waarin consistentiebeginselen zijn vastgesteld voor het goedkeuren en uitvoeren van de verzameling van inlichtingen uit berichtenverkeer, maar PPD-28 vormt geen rechtsgrondslag voor verzameling. PPD-28 bereikt zijn doel door deze beginselen op te leggen aan inlichtingendiensten, die deze moeten doorvoeren in hun beleid en procedures. De richtlijn is van toepassing op activiteiten op het gebied van inlichtingen uit berichtenverkeer, ongeacht of de gegevens zich op het moment dat ze worden verzameld binnen of buiten de Verenigde Staten bevinden. De richtlijn is daarom ook van toepassing op gegevens die ten behoeve van inlichtingen worden verzameld en daarbij worden doorgegeven van de EU naar de Verenigde Staten.

In het bijzonder geeft PPD-28 aan dat de activiteiten op het gebied van inlichtingen uit berichtenverkeer zo specifiek als haalbaar moeten zijn[40]. Met betrekking tot het gebruik van de gegevens legt PPD-28 procedures vast voor gegevensminimalisering (met inbegrip van voorwaarden voor het bewaren en verspreiden van de gegevens), gegevensbeveiliging en toegang voor relevant personeel [d.w.z. voorschriften die waarborgen bevatten om de risico's van misbruik en oneigenlijk gebruik beperken], gegevenskwaliteit en toezicht. Deze waarborgen zijn van toepassing ongeacht de nationaliteit van de betrokkenen, d.w.z. op Amerikanen en niet-Amerikanen.

Tijdens de doorgifte van de gegevens aan de Verenigde Staten zijn de door PPD-28 vastgestelde waarborgen ook van toepassing. Bijlage VI bevat een toezegging van het ODNI dat wanneer de Amerikaanse inlichtingendiensten gegevens verzamelen via trans-Atlantische kabels tijdens doorgifte van deze gegevens aan de Verenigde Staten, zij dat zouden doen onder toepassing van de beperkingen en waarborgen die in deze bijlage zijn vastgesteld, waaronder de vereisten van PPD-28[41]. WP29 merkt op dat er nog steeds een gebrek aan vaste rechtspraak is inzake de wettigheid van onderschepping via kabels door enig land. In elk geval bevestigen noch ontkennen de Verenigde Staten dat zij onderschepping via kabels gebruiken als middel voor het verzamelen van inlichtingen.

Het begrip "inlichtingen uit berichtverkeer" wordt niet gedefinieerd in PPD-28 noch in enige andere toepasselijke tekst.

3.2.2. Foreign Intelligence Surveillance Act

In het algemeen lijkt de tekst van de FISA duidelijker en nauwkeuriger. De interpretatie van veel bepalingen in het licht van PPD-28 en daarmee ook hun praktische toepassing zijn echter grotendeels afhankelijk van de uitvoering door de diverse instanties. Hoewel een volledig verslag van de uitvoering van de nieuwe waarborgen nog niet beschikbaar is, hebben

[40] "Activiteiten op het gebied van inlichtingen uit berichtenverkeer moeten zo specifiek als haalbaar zijn. Bij het vaststellen of zij inlichtingen uit berichtenverkeer zullen verzamelen, moeten de Verenigde Staten rekening houden met de beschikbaarheid van andere informatie, waaronder informatie uit diplomatieke en openbare bronnen. Dergelijke geschikte en uitvoerbare alternatieven voor inlichtingen uit berichtenverkeer moeten prioriteit krijgen." (paragraaf 1(d))

[41] Privacyschild bijlage VI, brief van het bureau van de directeur van de nationale inlichtingendienst (ODNI) met betrekking tot waarborgen en beperkingen die van toepassing zijn op de nationale veiligheidsautoriteiten van de Verenigde Staten, blz. 2.

Amerikaanse afgevaardigden vertegenwoordigers van WP29 ervan in kennis gesteld dat de uitvoering van de waarborgen van de PPD-28 voltooid is en deze uitvoering binnen de Amerikaanse inlichtingengemeenschap op een vergelijkbare manier plaatsvindt.

Meer bepaald is sectie 501 relatief duidelijk over het soort inlichtingenoperaties die onder mandaat kunnen worden gesteld: de productie van tastbare zaken (waaronder boeken, verslagen, artikels, documenten en andere zaken). Er moet echter worden opgemerkt dat het feit dat de definitie van "tastbare zaken", "andere zaken" omvat, de omvang van deze bevoegdheid vrij ruim maakt.

Artikel 702, dat het mogelijk maakt dat gegevens worden verzameld van niet-Amerikanen van wie redelijkerwijs wordt aangenomen dat zij buiten de Verenigde Staten verblijven, teneinde buitenlandse inlichtingen te verzamelen[42], treedt minder in detail dan sectie 501. Sectie 702 richt zich op in de Verenigde Staten gevestigde dienstverleners op het gebied van elektronische communicatie voor het verzamelen van buitenlandse inlichtingen over personen die buiten de Verenigde Staten verblijven. De definitie van "buitenlandse inlichtingen" is ruim. De definitie omvat onder andere informatie met betrekking tot een buitenlandse mogendheid of buitenlands grondgebied die verband houdt met het buitenlands beleid van de Verenigde Staten[43], hetgeen enige onzekerheid met zich meebrengt wat betreft het soort informatie dat in de praktijk kan worden verzameld.

Ondanks de opheffing van geheimhouding van documenten, verslagen aan het Congres en de toezichtsverslagen van de Privacy and Civil Liberties Oversight Board (hierna de "PCLOB" genoemd), blijft de toepassing van de FISA, inclusief de werkingssfeer en het gebruik van de specifieke selectietermen, onduidelijk en verwarrend. Naar het gebruik van specifieke selectietermen ("tasked selectors") wordt verwezen in een verslag van de PCLOB[44], maar WP29 is van mening dat dit niet overeenstemt met de specificeringsvoorschriften op grond van sectie 702[45]. Er wordt niet naar verwezen in algemeen toegankelijke voorschriften, voor zover WP29 heeft kunnen nagaan.

3.2.3 Conclusie

In het algemeen merkt WP29 op dat de toepasselijke teksten met betrekking tot inlichtingenactiviteiten online beschikbaar zijn en dat de Amerikaanse autoriteiten een aantal belangrijke stappen hebben gezet voor meer transparantie.

WP29 erkent dat sinds 2013 een groot aantal documenten zoals beleidsstukken, procedures, FISC-beslissingen en andere vrijgegeven documenten is gepubliceerd. Bovendien heeft de PCLOB belangrijke verslagen uitgebracht over de activiteiten die worden uitgevoerd op basis van sectie 702 en de USA FREEDOM ACT. Een vergelijkbaar verslag wordt verwacht over activiteiten in het kader van EO12333.

[42] 50 U.S. Code §1881a (D)(1).
[43] 50 U.S. Code § 1801 (e) (2).
[44] PCLOB-verslag over het toezichtsprogramma dat wordt uitgevoerd overeenkomstig sectie 702 FISA, blz. 32.
[45] 50 U.S. Code § 1881a(D).

Verschillende wetgevende bijlagen die licht zouden kunnen werpen op de gevolgen van het uitvoeringsbesluit voor personen buiten de Verenigde Staten en alle toepasselijke waarborgen zijn geheim en als zodanig niet toegankelijk voor het publiek of personen die mogelijk worden getroffen door de toepassing daarvan. De teksten die wel zijn vrijgegeven, zijn maar van beperkte waarde en bieden slechts beperkt inzicht in de inlichtingenactiviteiten.

Ondanks de inspanningen die na de onthullingen van Snowden zijn gedaan om de werking van EO12333 uit te leggen, in het bijzonder door middel van de aanneming van PPD-28, blijft de huidige praktische toepassing van EO12333 onduidelijk. WP29 merkt op dat bijlage VI bij het privacyschild geen gedetailleerde informatie verstrekt over de werking van EO12333.

WP29 verwelkomt de beperkingen van PPD-28, maar het blijft moeilijk om te bepalen of het Amerikaanse rechtskader voor toezicht voldoende voorzienbaar is, d.w.z. adequate aanwijzingen bevat over de omstandigheden waarin en de voorwaarden waaronder overheden hun toevlucht mogen nemen tot zulke maatregelen. Het is nog wachten op verdere opheldering met onder meer de publicatie van het verslag van de PCLOB inzake EO12333.

3.3 Waarborg B - Noodzakelijkheid en evenredigheid moeten worden aangetoond met betrekking tot de legitieme nagestreefde doeleinden

3.3.1 Presidentiële beleidsrichtlijn 28

PPD-28 heeft beperkingen ingevoerd met betrekking tot de doelen waarvoor persoonsgegevens kunnen worden gebruikt en de voorwaarden waaronder zij kunnen worden verspreid, en heeft invloed op de verzameling van inlichtingen via berichtenverkeer, ongeacht de rechtsgrondslag die wordt gebruikt.

In het bijzonder bepaalt sectie 1 van PPD-28 dat Amerikaanse activiteiten op het gebied van inlichtingen uit berichtenverkeer altijd zo specifiek als haalbaar moeten zijn. Deze beperking wordt erkend, maar het is moeilijk vast te stellen of "zo specifiek als haalbaar" betekent dat alle gegevensverzameling noodzakelijk en evenredig is.

PPD-28 erkent dat bulksgewijze verzameling toegestaan blijft om nieuwe of opkomende dreigingen en andere voor de nationale veiligheid essentiële informatie te identificeren die vaak onopgemerkt blijven binnen het grote en complexe systeem van moderne wereldwijde communicatie[46]. WP29 merkt op dat PPD-28 aangeeft dat het bulksgewijs verzamelen van inlichtingen uit berichtenverkeer de toegestane verzameling betekent van grote hoeveelheden inlichtingen uit berichtenverkeer die, om technische of operationele overwegingen, plaatsvindt zonder gebruikmaking van discriminanten (bv. specifieke voorzieningen, selectietermen, enz.).

PPD-28 legt beperkingen op aan het gebruik van bulksgewijs verzamelde inlichtingen uit berichtenverkeer met betrekking tot het gebruiksdoel. Tot de zes doelen waarvoor bulksgewijs

[46] PPD-28, sectie 2 en bijlage VI bij het privacyschild, de brief van het bureau van de directeur van de nationale inlichtingendienst (ODNI) met betrekking tot waarborgen en beperkingen die van toepassing zijn op de nationale veiligheidsautoriteiten van de Verenigde Staten, blz. 3.

gegevens kunnen worden verzameld, behoren onder meer terrorismebestrijding en andere vormen van ernstige (internationale) misdaad. De analyse van WP29 wijst erop dat de doelbinding tamelijk ruim is (en mogelijk te ruim) om als gericht te worden beschouwd.

PPD-28 heeft de mogelijkheid voor ongedifferentieerde bulksgewijze verzameling van persoonsgegevens behouden en de omvang van deze verzamelmogelijkheid blijft onduidelijk en mogelijk groot. Dienaangaande merkt WP29 op dat ODNI in bijlage VI bevestigt dat bulksgewijze verzamelingsactiviteiten met betrekking tot internetcommunicatie die de Amerikaanse inlichtingendiensten door middel van inlichtingen uit berichtenverkeer uitvoeren, betrekking hebben op een klein deel van het internet[47]. WP29 zou op dit gebied verder bewijs door middel van transparantiemaatregelen op prijs stellen.

3.3.2. Foreign Intelligence Surveillance Act

Sectie 215 en sectie 702 FISA minimalisatieprocedures zijn geïntroduceerd teneinde Amerikaanse burgers te beschermen tegen verreikende toegang door de regering tot hun gegevens. Deze beperkingen zijn niet officieel van toepassing op buitenlanders, hoewel Amerikaanse regeringsfunctionarissen herhaaldelijk zowel in openbare als in besloten vergaderingen met vertegenwoordigers van WP29 hebben aangegeven dat het toepassingsgebied van de minimalisatieprocedures in de praktijk is uitgebreid naar alle personen, ongeacht hun nationaliteit of gebruikelijke verblijfplaats.

Sectie 702 specificeert dat toegestane gegevensverzameling plaatsvindt overeenkomstig het Vierde amendement op de grondwet van de Verenigde Staten dat gegevensverzameling beperkt tot wat als overeenkomstig met het redelijke zoekbeginsel wordt beschouwd, en dat wat dit betreft er geen verschil wordt gemaakt tussen Amerikaanse en niet-Amerikaanse bedrijven. Dit houdt in dat als het Vierde amendement van toepassing was op alle in de Verenigde Staten verzamelde gegevens, bulksgewijze verzameling daar onredelijk en bijgevolg ongrondwettelijk zou zijn.

WP29 is verheugd over de bevindingen in het verslag van PCLOB dat in de praktijk ook niet-Amerikanen profiteren van de beperkingen op het gebied van toegang en bewaring, vereist onder de minimaliserings- en/of specificeringsprocedures van de diverse instanties als gevolg van de kosten, en problemen bij het identificeren en verwijderen van persoonlijke informatie in de Verenigde Staten voor een grote hoeveelheid gegevens er doorgaans toe leiden dat de volledige reeks gegevens wordt behandeld in overeenstemming met de hogere Amerikaanse gegevensnormen.

WP29 merkt verder op dat volgens de bevindingen van PCLOB het programma niet functioneert door middel van het bulksgewijs verzamelen van communicatie. Het 2014

[47] Bijlage VI bij het Privacyschild, de brief van het bureau van de directeur van de nationale inlichtingendienst (ODNI) met betrekking tot waarborgen en beperkingen die van toepassing zijn op Amerikaanse nationale veiligheidsdiensten, blz. 4; WP29 herinnert in dit opzicht aan het verslag over de bevindingen van de EU-medevoorzitters van de ad hoc EU-VS werkgroep gegevensbescherming, dat aangeeft dat communicatiegegevens een heel klein deel uitmaken van het wereldwijde internetverkeer, aangezien het meeste wereldwijde internetverkeer bestaat uit hoog-volume streaming en downloads zoals televisieseries, films en sport (§ 3.1.2 van het verslag)44.

Statistical Transparency Report van het ODNI bevestigt deze bevinding. Bovendien worden volgens het PCLOB-verslag ten behoeve van gericht toezicht "tasked selectors" gebruikt, zoals een e-mailadres of een telefoonnummer[48].

De overeenkomstige beschikbare openbare voorschriften met betrekking tot de specificering van doelwitten voorzien echter niet in dergelijke gerichte voorschriften en trachten uitsluitend te voorkomen dat Amerikaanse burgers of in de Verenigde Staten gevestigde personen als doelwit worden gespecificeerd. Bovendien zijn de voordelen die volgens PCLOB van toepassing zijn op niet-Amerikanen in de praktijk niet juridisch bindend of wettelijk vastgelegd, aangezien de beschikbare wetgeving met betrekking tot het specificeren van doelwitten niet voorziet in dergelijke gerichte voorschriften en uitsluitend tracht te voorkomen dat Amerikaanse burgers of in de Verenigde Staten gevestigde personen als doelwit worden gespecificeerd.

WP29 herinnert er bovendien aan dat ten behoeve van sectie 702 personen niet alleen individuen zijn, maar ook groepen, entiteiten, associaties, ondernemingen, of buitenlandse mogendheden. Bovendien laat het feit dat verzameling gerechtvaardigd is doordat het verkrijgen van buitenlandse inlichtingen een significant doel van de verwerving is, enige onzekerheid bestaan met betrekking tot het doel en de noodzaak ervan. WP29 verwelkomt echter de in bijlage VI verstrekte informatie dat het totale aantal personen dat in 2014 krachtens sectie 702 als doelwit is gespecificeerd, ongeveer 90 000 personen bedroeg[49]. De eerste herziening van het privacyschild zal een mogelijkheid bieden voor meer bewijzen van de specificatievoorschriften die moeten worden aangetoond.

Tot nu toe is er geen afdoende rechtspraak over de wettigheid van de grootschalige en ongedifferentieerde gegevensverzameling en het daaropvolgend gebruik van persoonsgegevens ten behoeve van criminaliteitsbestrijding en de vraag onder welke omstandigheden deze verzameling en dit gebruik kunnen plaatsvinden. Naar verwachting zal het HvJEU deze kwestie althans tot op zekere hoogte bespreken in de loop van 2016, zowel in de gevoegde zaken Tele2 Sverige AB/Post-och telestyrelsen en Secretary of State for the Home Department/Davis en anderen[50] als in het uit te brengen advies over de geldigheid van de PNR-overeenkomst met Canada[51]. In tussentijd herinnert WP29 eraan dat zij steeds van mening is geweest dat grootschalige en ongedifferentieerde verzameling van gegevens in elk geval niet als evenredig kan worden beschouwd[52].

3.3.3 Conclusie

Ondanks de beperkingen naar aanleiding van de invoering van PPD-28, blijft WP29 bezorgd, in het bijzonder met betrekking tot de evenredigheid van de gegevensverzameling. In de eerste plaats zijn er aanwijzingen dat de Verenigde Staten blijven doorgaan met grootschalige

[48] PCLOB-verslag over het toezichtsprogramma dat wordt uitgevoerd overeenkomstig sectie 702 FISA, blz. 32.
[49] Bijlage VI, blz. 11.
[50] HvJEU, gevoegde zaken C-203/15 en C-698/15.
[51] HvJEU, zaak A-1/15.
[52] WP215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_nl.pdf

en ongedifferentieerde gegevensverzameling, of dat ze in ieder geval niet uitsluiten dat zij in de toekomst nog op zulke wijze gegevens zullen verzamelen. WP29 heeft steeds volgehouden dat deze wijze van gegevensverzameling niet in overeenstemming is met het EU-recht en daarom onaanvaardbaar is.

Ten tweede merkt WP29 op dat ook gerichte gegevensverwerking, of verwerking die "zo specifiek als haalbaar" is, nog steeds als grootschalig kan worden beschouwd. De vraag of het op grote schaal verzamelen van gegevens moet worden toegestaan of niet, maakt thans het voorwerp uit van een procedure voor het HvJEU. Om deze reden zal WP29 geen definitieve beoordeling geven inzake de wettigheid van gerichte maar grootschalige gegevensverwerking. Zij benadrukt echter dat indien gerichte maar grootschalige gegevensverwerking zou worden toegestaan, de specificeringsbeginselen van toepassing zouden moeten zijn op zowel de verzameling als het daaropvolgende gebruik van gegevens, en niet kunnen worden beperkt tot enkel het gebruik. In elk geval is nadere toelichting van het ontwerp-adequaatheidsbesluit nodig met betrekking tot de zes in PPD-28 genoemde doelen waarvoor gegevens in bulk kunnen worden verzameld. WP29 is er in deze fase niet van overtuigd dat deze doelen voldoende zijn ingeperkt om te waarborgen dat de gegevensverzameling daadwerkelijk beperkt wordt tot wat noodzakelijk en evenredig is.

3.4 Waarborg C - Er moet een onafhankelijk toezichtsmechanisme zijn

De Verenigde Staten beschikken niet over één enkel toezichtsorgaan op federaal niveau dat als taak heeft toezicht te houden op de gevolgen van inlichtingen- en toezichtprogramma's voor privacy en gegevensbescherming. De inlichtingenactiviteiten van de Verenigde Staten worden onderworpen aan een pluriform toezichtsproces: er kan onderscheid worden gemaakt tussen intern en extern toezicht. WP29 erkent dat de rapportagepraktijk van de Amerikaanse toezichtsorganen zeer gedetailleerd en grotendeels openbaar is.

3.4.1 Intern toezicht

Alle inlichtingen- en veiligheidsinstanties beschikken over personeel dat verantwoordelijk is voor het waarborgen van naleving van hun wetgevend kader, inclusief inspecteurs-generaal wier primaire taak het is om de algehele naleving te beoordelen van het werk van de instanties met de wetgeving onder meer op het gebied van privacy en gegevensbescherming. De inspecteurs-generaal worden bij wet aangesteld en zijn (of worden binnenkort) allemaal benoemd door de president gevolgd door een goedkeuring door de Senaat, hetgeen ervoor moet zorgen dat zij organisatorisch onafhankelijk zijn en rapporteren aan het Congres. WP29 is van mening dat gezien het bovenstaande de inspecteurs-generaal waarschijnlijk zullen voldoen aan het criterium van organisatorische onafhankelijkheid zoals gedefinieerd door het HvJEU en het Europees Hof voor de rechten van de Mens (EHRM), ten minste vanaf het moment dat de nieuwe benoemingsprocedure op iedereen van toepassing wordt. Voorlopig blijft een aantal zorgen bestaan met betrekking tot inspecteurs-generaal die nog worden benoemd door de directeur van de instantie waarop zij toezicht houden.

De inspecteurs-generaal kunnen aanbevelingen doen die vervolgens kunnen worden doorgestuurd naar het ministerie van Justitie en de PCLOB of zelfs naar het Amerikaanse Congres, die de aanbevelingen ten uitvoer kunnen leggen. Als de inspecteur-generaal een overtreding vaststelt, kan die worden aangepakt via interne en beleidsmaatregelen en worden gerapporteerd aan het Congres. De inspecteur-generaal heeft bijvoorbeeld de bevoegdheid om audits en inspecties uit te voeren.

WP29 merkt op dat de verslagen van de inspecteur-generaal voor het publiek geheim kunnen worden gehouden en dat kan worden beslist dat een inspecteur-generaal niet hoeft te rapporteren als de onderzochte informatie als geheim wordt aangemerkt. De verslagen zullen echter te allen tijde worden onderworpen aan toezicht door het Congres, hetgeen een essentiële waarborg is, hoewel het niet voorziet in een individuele verhaalmogelijkheid.

Alle instanties beschikken over functionarissen op het gebied van privacy en burgerlijke vrijheden die helpen met het verplichte zelfrapportagesysteem met toezicht van het Congres.

In het algemeen kunnen de bestaande interne toezichtsmechanismen als tamelijk solide worden beschouwd; om inmenging in de grondrechten inzake privacy en gegevensbescherming te rechtvaardigen, moet het toezicht echter volledig onafhankelijk zijn. Hoewel WP29 het werk van de verschillende functionarissen op het gebied van privacy en burgerlijke vrijheden respecteert en waardeert, kan zij niet concluderen dat deze functionarissen voldoen aan het vereiste niveau van onafhankelijkheid om op te treden als onafhankelijk toezichthouder.

3.4.2 Extern toezicht

Extern toezicht vindt plaats via een aantal verschillende mechanismen: gerechtelijk toezicht krachtens de secties 501 en 702 gegarandeerd door de FISA-rechtbank (hierna "FISC" genoemd), het toezicht van de Select Intelligence Committees van het Congres en de door de PCLOB uitgevoerde taken.

WP29 herinnert eraan dat het toezicht bij voorkeur, zoals ook al werd aangegeven door het HvJEU en het EHRM, in handen zou moeten zijn van een rechter, teneinde de onafhankelijkheid en onpartijdigheid van de procedure te garanderen. Tot voor kort was de FISC-procedure een ex parte procedure waarbij de betrokkenen niet konden worden gehoord of zelfs niet op de hoogte konden worden gebracht van het bestaan van de zaak. Ook nu is de FISC-procedure nog ex parte, maar na de goedkeuring van de USA FREEDOM ACT zijn de amici curiae in het kader van de FISC ingevoerd. De amici curiae werken onafhankelijk, maar zijn niet aangesteld om specifieke personen te verdedigen die bij een zaak betrokken kunnen zijn.

De USA Freedom Act heeft een groep amici curiae in het leven geroepen om de FISC in te lichten over belangrijke zaken. De rechtbank heeft vijf advocaten geselecteerd die de passende veiligheidsmachtigingen hebben verkregen en technisch advies verlenen, hoorzittingen van de FISC bijwonen en resumés leveren, en argumenteren over de grond van

een zaak vanuit een perspectief van privacy en burgerrechten. Zij zullen dit echter alleen doen in belangrijke zaken of in geval van nieuwe juridische vragen[53].

Sectie 215 staat bijna volledig onder ex ante (maar niet ex post) gerechtelijk toezicht, aangezien alle programma's die sectie 215 gebruiken als basis voor verzameling onderworpen zijn aan goedkeuring door de FISC. Het verslag van de PCLOB specificeert dat "sectie 702 verschilt van dit traditionele elektronische toezichtskader van de FISA zowel wat betreft de toegepaste normen als het gebrek aan geïndividualiseerde vaststellingen door de FISC. Volgens de wet maken de Attorney General en de Director of National Intelligence jaarlijks certificeringen die het specificeren toelaten van niet-Amerikanen van wie redelijkerwijs kan worden aangenomen dat zij zich buiten de Verenigde Staten bevinden, om buitenlandse inlichtingen te vergaren, zonder aan de FISC te specificeren welke specifieke niet-Amerikaanse onderdanen als doelwit zullen worden gespecificeerd. [...] Er is ook geen vereiste dat de regering de mogelijke reden aantoont waarom kan worden aangenomen dat een doelwit onder sectie 702 een buitenlandse mogendheid of vertegenwoordiger van een buitenlandse mogendheid is, zoals is vereist onder de oorspronkelijke FISA.[54]"

Binnen het Congres hebben de Select Intelligence Committees ook een toezichthoudende taak en keuren zij inlichtingenactiviteiten goed, in het bijzonder via stemming over de begroting. Senate and House Intelligence Committees ontvangen geheime briefings over inlichtingenactiviteiten. De Attorney General moet elke zes maanden aan deze Committees verslag uitbrengen over het elektronisch toezicht van de FISA. Het blijft onduidelijk voor WP29 in welke mate zij de verwerking van persoonsgegevens van individuele personen, in het bijzonder niet-Amerikanen, kunnen bespreken.

De PCLOB is een onafhankelijk onderdeel van de uitvoerende macht in de Amerikaanse regering en heeft twee fundamentele bevoegdheden: (1) controleren en analyseren van de acties die de uitvoerende macht neemt om de Verenigde Staten te beschermen tegen terrorisme en er daarbij voor zorgen dat de noodzaak van dergelijke acties in verhouding staat tot de noodzaak de privacy en burgerlijke vrijheden te beschermen, en (2) waarborgen dat kwesties inzake vrijheden naar behoren in aanmerking worden genomen bij de ontwikkeling en tenuitvoerlegging van wetgeving, regelgeving en beleid met betrekking tot inspanningen om het land tegen terrorisme te beschermen. WP29 merkt op dat de PCLOB de macht heeft om te dagvaarden en toegang heeft tot geheime informatie. Tijdens de uitvoering van zijn taak controleert hij ook de doeltreffendheid van de programma's. Zijn toezicht wordt uitgevoerd na de feiten, niet voorafgaand. De PCLOB heeft zijn onafhankelijke macht aangetoond door met de president van de Verenigde Staten van mening te verschillen inzake juridische kwesties. In het bijzonder stelde de PCLOB vast dat het programma inzake telefoonmetagegevens van sectie 215 niet wettelijk was toegestaan en goedgekeurd en concludeerde dat het niet doeltreffend was aangezien er geen bewijzen waren van aanvallen met verstorende werking. De PCLOB heeft ook een jaar lang onderzoek gevoerd naar het 702-programma en oordeelde dat het juridisch en duidelijk bij wet is toegestaan en dat sectie 702 zeer doeltreffend is

[53] Freedom Act TITLE IV--FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS Sec. 401. Appointment of amici curiae.
[54] PCLOB-verslag over het toezichtsprogramma dat wordt uitgevoerd overeenkomstig sectie 702 FISA, blz. 24 en 25.

gebleken, onder andere met betrekking tot terrorismekwesties. Ten slotte onderzocht de PCLOB de transparantievereiste en stelde hij vast dat een aantal als geheim aangemerkte feiten niet als dusdanig hoefde te worden geclassificeerd. De PCLOB zal naar verwachting in de nabije toekomst verslag uitbrengen over de uitvoering van PPD-28. Wat dat betreft, is de PCLOB van mening dat om informatie over een buitenlander te behouden, het simpele feit dat die persoon buitenlander is, niet volstaat.

WP29 merkt ten slotte op dat EO12333 niet voorziet in enige gerechtelijke toetsing, toezicht of verhaalmechanismen voor de op grond van EO12333 uitgevoerde toezichtsprogramma's.

3.4.3 Conclusie

Het ontwerp-adequaatheidsbesluit toont aan dat een pluriforme aanpak van zowel interne als externe toezichtsmechanismen in de Verenigde Staten aanwezig is. Hoewel de werking van de toezichtsmechanismen verwarrend kan zijn, is WP29 tevreden dat, in het algemeen, voldoende interne toezichtsmechanismen aanwezig zijn. WP29 is echter bezorgd dat er onvoldoende toezicht is op de toezichtsprogramma's die worden uitgevoerd op basis van EO12333.

WP29 merkt op dat haar eerdere kritiek dat de procedures voor de FISC niet contradictoir zijn, maar in beperkte mate is gematigd door de invoering van de amici curiae die tot taak hebben de bescherming van individuele privacy en burgerlijke vrijheden te bevorderen. Toch voorziet de FISC niet in doeltreffend gerechtelijk toezicht op het als doelwit specificeren van niet-Amerikanen. Er blijven ook enige twijfels bestaan met betrekking tot het vermogen van de FISC om de specificerings- en minimaliseringsprocedures te beoordelen, zoals ook is aangegeven door de PCLOB[55].

3.5 Waarborg D - Individuen moeten toegang hebben tot doeltreffende rechtsmiddelen

3.5.1 Beroepsmogelijkheden

3.5.1.1 Vereiste van procesbevoegdheid

Het Amerikaanse systeem met betrekking tot hoger beroep heeft een belangrijke beperking: de Amerikaanse grondwet vereist dat een persoon aantoont dat hij procesbevoegdheid heeft: "de eis dat aanklagers rechtstreeks letsel of schade hebben geleden of zullen lijden en dat deze schade verhaalbaar is. Op federaal niveau kunnen rechtszaken niet worden aangespannen eenvoudigweg omdat een persoon of groep niet tevreden is met het optreden van de regering of een wet.[56]" Deze vereiste lijkt teniet te worden gedaan door het gebrek aan kennisgeving aan personen die zijn onderworpen aan toezicht, zelfs nadat de maatregelen zijn geëindigd. Het HvJEU en het EHRM hebben herhaaldelijk aangegeven dat personen toegang moeten hebben tot administratieve of gerechtelijke beroepsmogelijkheden. Het EHRM heeft in zijn Zakharov-arrest bevestigd dat op basis van de rechtspraak iedereen naar de rechter kan

[55] PCLOB-verslag over het toezichtsprogramma dat wordt uitgevoerd overeenkomstig sectie 702 FISA, blz. 11.
[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standinghttps://www.law.cornell.edu/wex/standing; Clapper/Amnesty International USA.

stappen als hij of zij een gerechtvaardigde reden heeft om inmenging in zijn of haar grondrechten te vermoeden[57].

Bovendien wordt aan buitenlanders die buiten de Verenigde Staten wonen, in de Verenigde Staten geen volledige constitutionele bescherming geboden, volgens rechtspraak van het Hooggerechtshof van de Verenigde Staten[58]. Dit geldt in het bijzonder met betrekking tot het Vierde amendement, dat Amerikaanse burgers – maar geen niet-Amerikanen – beschermt tegen onredelijk huiszoekingen en inbeslagnemingen, en waarvan een groot deel van het Amerikaanse recht op privacy is afgeleid. Europese burgers en andere Europese personen die buiten de Verenigde Staten wonen, worden eenvoudigweg uitgesloten van de bescherming van het Vierde amendement[59].

De beperkte toepassing van de Judicial Redres Act (zowel qua inhoud omdat deze geen betrekking heeft op nationale veiligheid, maar ook wat betreft de personen die zich erop kunnen beroepen), de vele uitzonderingen en de juridische onzekerheid met betrekking tot de instanties waarop de Judicial Redres Act van toepassing is, zijn niet in overeenstemming met de vereiste om een doeltreffend verhaalmechanisme te bieden aan alle betrokken personen in toezichtszaken van nationale veiligheid en inlichtingen.

3.5.1.2 Presidentiële beleidsrichtlijn 28

WP29 merkt op dat PPD-28 slechts een richtlijn is en daarom geen rechten voor natuurlijke personen kan doen ontstaan. Dat kan alleen door middel van wetgeving gebeuren. Dit betekent dat personen niet naar de rechter kunnen stappen op basis van een vermeende schending van de waarborgen van PPD-28.

3.5.1.3 Foreign Intelligence Surveillance Act

Krachtens de FISA bestaan er enkele rechtsmiddelen voor personen in het geval van onrechtmatig toezicht. Volgens de FISA heeft een benadeelde die geen buitenlandse mogendheid of vertegenwoordiger van een buitenlandse mogendheid is, en die is onderworpen aan elektronisch toezicht of over wie door middel van elektronisch toezicht informatie is verkregen die openbaar is gemaakt of is gebruikt in strijd met sectie 1809, een grond voor beroep tegen elke persoon die deze schending pleegde. Hiermee wordt de aan de maatregel onderworpen buitenlandse mogendheid of vertegenwoordiger van een buitenlandse mogendheid echter nadrukkelijk uitgesloten. Toch zal de klager, zoals reeds aangegeven, moeten aantonen dat hij procesbevoegdheid heeft, hetgeen niet mogelijk zal zijn in de praktijk.

De USA Freedom Act heeft een Amicus Curiae-adviescommissie in het leven geroepen bij de FISA-rechtbank om (facultatief) advies te geven in het geval van een belangrijke, nieuwe juridische interpretatie. De taak van de adviescommissie is echter om onbevooroordeeld

[57] EHRM, Zakharov, §171.
[58] Verenigde Staten/Verdugo - Urquidez, blz. 264-266.
[59] Verslag van de EU-medevoorzitters, sectie 2.

advies te geven, en niet om het belang van een specifiek persoon op zijn/haar verzoek te verdedigen.

3.5.2 Bestuurlijke rechtsmiddelen

3.5.2.1 Inspecteurs-generaal

Een andere mogelijkheid voor verhaal is via de inspecteur-generaal bij wie een klacht kan worden ingediend. Inspecteurs-generaal zijn echter niet verplicht om elke afzonderlijke klacht te onderzoeken: er is geen recht om te worden gehoord, maar eerder een discretionaire bevoegdheid. De inspecteur-generaal kan ook verslagen uitbrengen met bevindingen van schendingen als informatie wordt vrijgegeven. Ingeval een persoon kan aannemen dat het verslag hem treft, zou hij vervolgens naar de rechter kunnen stappen op basis van de bevinding van de inbreuk op de wet.

3.5.2.2 Freedom of Information Act

Een beroepsmogelijkheid die voor alle personen beschikbaar is, is het indienen van een verzoek om het vrijgeven van informatie, op basis van de Freedom of Information Act (FOIA). Volgens de Amerikaanse regering kan een FOIA-verzoek worden ingediend door over het algemeen elke persoon – Amerikaans burger of niet – louter door te vragen om een document van de instantie. Het kan gaan om documenten over de persoon, al moet in dat geval een bewijs van identiteit worden voorgelegd. Als informatie echter als geheim is aangemerkt om de nationale veiligheid te beschermen, zal een FOIA-verzoek waarschijnlijk weinig succes kennen, aangezien er een uitzondering van toepassing is: instanties zijn niet verplicht om toegang te verschaffen tot geheime informatie, ook niet als deze informatie betrekking heeft op de persoon die het verzoek indient. Informatie van lopende rechtshandhavingsonderzoeken is volledig uitgesloten van FOIA-verzoeken. Ten slotte verschaft het FOIA-verzoek volgens WP29 geen recht om de rechtmatigheid van de verwerking te laten controleren door een onafhankelijke instantie.

3.5.3 Ombudsman van het privacyschild

3.5.3.1 Instelling van een ombudsman

Het privacyschild biedt een nieuw mechanisme waarmee "natuurlijke personen in de EU" bij de onlangs ingestelde ombudsman van het privacyschild verzoeken kunnen indienen met betrekking tot "Amerikaanse inlichtingen uit berichtenverkeer". De positie van de ombudsman zal, zoals uiteengezet in het bij de brief van Minister van Buitenlandse Zaken John Kerry van 22 februari 2016 gevoegde memorandum, worden bekleed door staatssecretaris C. Novelli. Zij zal deze bij artikel 4, onder d), van PPD-28 ingestelde functie vervullen naast haar rol als de "Senior Coordinator for International Information Technology Diplomacy". In de brief en in het memorandum wordt benadrukt dat de staatssecretaris "rechtstreeks verslag uit[brengt] aan de Minister van Buitenlandse Zaken" en "onafhankelijk van de inlichtingendiensten" is.

In het memorandum wordt uitgelegd dat, ondanks zijn benaming, de ombudsman van het privacyschild niet alleen verzoeken zal behandelen inzake de toegang uit hoofde van de nationale veiligheid tot vanuit de EU naar de VS in het kader van het privacyschild doorgegeven gegevens, maar ook verzoeken waarbij de gegevens zijn doorgegeven overeenkomstig modeldcontractbepalingen, bindende bedrijfsvoorschriften, afwijkingen (als bedoeld in artikel 26 van Richtlijn 95/46/EG) of "mogelijke toekomstige afwijkingen", als gedefinieerd in voetnoot 2 van het memorandum.

De manier waarop het mechanisme dient te werken, kan als hierna volgt worden samengevat. Een natuurlijke persoon in de EU dient een verzoek in bij een instantie van een lidstaat die bevoegd is om toezicht op nationale veiligheidsdiensten uit te oefenen, of bij een "centraal EU-orgaan voor de behandeling van individuele klachten", in het geval een dergelijke instantie wordt ingesteld of aangewezen. De autoriteit die het verzoek doorstuurt naar de ombudsman moet eerst controleren of het verzoek volledig is, in de zin van punt 3, onder b), van de brief.[60] Wanneer het verzoek is doorgestuurd naar de ombudsman van het privacyschild en in overeenstemming met punt 3, onder b), is bevonden, zal de ombudsman van het privacyschild een antwoord sturen. Daarbij bevestigt hij dat (i) "de klacht naar behoren is onderzocht, en (ii) dat is voldaan aan de wetgeving van de VS, uitvoeringsbevelen, presidentiële richtlijnen en beleidsmaatregelen van instanties die voorzien in de beperkingen en waarborgen die worden beschreven in de brief van het bureau van de directeur van de nationale inlichtingendienst (Office of the Director of National Intelligence (ODNI)), of, indien er sprake is van niet-naleving, dat deze niet-naleving is verholpen."[61] Het antwoord zal "bevestigen noch ontkennen dat de betrokkene het voorwerp is geweest van surveillance, noch zal de privacyschild-ombudsman de specifieke oplossing bevestigen die werd gekozen."[62] Met betrekking tot de wijze van onderzoek door de ombudsman, wordt toegelicht dat "de privacyschild-ombudsman "nauw [zal] samenwerken met andere regeringsambtenaren van de Verenigde Staten, waaronder passende daarvoor in aanmerking komende toezichthoudende organen"[63], en met name "nauw [zal] kunnen samenwerken met het bureau van de directeur van de nationale inlichtingendienst, het ministerie van Justitie en andere ministeries en agentschappen die in voorkomend geval betrokken zijn bij de nationale veiligheid van de Verenigde Staten, en met inspecteurs-generaal, ambtenaren die met de uitvoering van de Freedom of Information Act zijn belast en ambtenaren op het gebied van

[60] b. De EU-instantie voor de behandeling van individuele klachten zal er, door middel van de volgende handelingen, op toezien dat het verzoek volledig is:
(i) door de identiteit van het individu te controleren en door te controleren of de persoon in eigen naam handelt en niet als vertegenwoordiger van een gouvernementele of een intergouvernementele organisatie;
(ii) door erop toe te zien dat het verzoek schriftelijk wordt gedaan en dat het de volgende basisinformatie bevat:
• alle informatie die de basis vormt voor het verzoek,
• de aard van de informatie of het gewenste herstel,
• de overheidsorganen van de Verenigde Staten die eventueel geacht worden betrokken te zijn, en
• de andere maatregelen die zijn genomen om de gevraagde informatie of het gevraagde herstel te verkrijgen en het naar aanleiding van die andere maatregelen ontvangen antwoord;
(iii) door te controleren of het verzoek betrekking heeft op gegevens die redelijkerwijs worden verondersteld uit de EU te zijn doorgegeven naar de Verenigde Staten op grond van het privacyschild, modelcontractbepalingen, bindende bedrijfsvoorschriften, afwijkingen, of mogelijke toekomstige afwijkingen;
(iv) door het doen van een eerste vaststelling dat het verzoek niet lichtzinnig, vexatoir, of te kwader trouw werd gedaan.
[61] Privacyschild bijlage III, punt 4, onder e)
[62] Privacyschild bijlage III, punt 4, onder e)
[63] Privacyschild bijlage III, punt 2, onder a)

burgerlijke vrijheden en privacy"[64]. Deze samenwerking zal zodanig zijn dat zij waarborgt dat de ombudsman van het privacyschild een antwoord kan sturen dat de hierboven beschreven bevestigingen bevat.

3.5.3.2 De beoordeling van het nieuwe ombudsmanmechanisme

De werkgroep erkent de inspanningen van de Europese Commissie en de Amerikaanse regering om een nieuw mechanisme te introduceren dat de verhaalsmogelijkheden met betrekking tot Amerikaanse toezichtsactiviteiten moet verbeteren. Zij begrijpt dat de beoordeling van dit mechanisme, als een noviteit binnen de internationale betrekkingen op het gebied van inlichtingen uit berichtenverkeer of nationale veiligheid, van bijzonder belang is.

In dit onderdeel zal WP29 beoordelen hoe de instelling van een ombudsman van het privacyschild zich verhoudt tot de in het Handvest, het EVRM en de jurisprudentie van de Europese rechters neergelegde vereisten waaraan moet zijn voldaan, willen natuurlijke personen hun verhaalsrecht kunnen uitoefenen.

3.5.3.3 Kan de instelling van een ombudsman op zich voldoende zijn?

Om te beginnen moet worden betwijfeld of de instelling van een "ombudsman" ooit geacht kan worden in overeenstemming te zijn met artikel 47 van het Handvest - dat spreekt van een doeltreffende voorziening in rechte en een onpartijdig gerecht[65] - ten minste als er geen andere weg beschikbaar is om doeltreffend beroep in te stellen. Dit is belangrijk omdat het HvJEU in zijn belangrijke overweging 95 in het arrest Schrems verwijst naar artikel 47 van het Handvest, en dit doet zonder enige indicatie dat artikel 47 in de context van toezichtsmaatregelen anders moet worden opgevat. Integendeel, het HvJEU paste artikel 47 van het Handvest al in de Kadi II-zaak[66] toe op toezichtsmaatregelen in verband met de nationale, respectievelijk internationale veiligheid[67].

De jurisprudentie van het EHRM maakt het echter heel duidelijk dat het recht om beroep in te stellen bij de gewone rechter geen voorwaarde is om toezichtsregelingen in overeenstemming met artikel 8 (en artikel 13) van het EVRM te kunnen achten.[68] Het EHRM heeft juist gepreciseerd dat krachtens artikel 8 de mogelijkheid bij andere autoriteiten beroep in te stellen een noodzakelijke waarborg in het kader van toezichtsactiviteiten kan zijn. Het EHRM heeft desondanks hoge verwachtingen van andere instanties die een doeltreffende beroepsmogelijkheid bieden, en geeft aan dat een dergelijke instantie "onafhankelijk moet

[64] Privacyschild bijlage III, punt 2, onder a)
[65] In de Toelichtingen bij het Handvest van de grondrechten wordt bovendien verklaard dat artikel 47 zo moet worden uitgelegd dat dit het recht op een doeltreffende voorziening in rechte
waarborgt (Toelichting bij het Handvest van de grondrechten, toelichting bij artikel 47 (2007/C 303/02)).
[66] Gevoegde zaken C-584/10 P, C-593/10 P en C-595/10 P, Europese Commissie en Verenigd Koninkrijk/ Kadi, 18 juli 2013
[67] Arrest Kadi II, punten 97 en 100: de rechtmatigheid van alle handelingen van de Unie, met inbegrip van die welke zijn bedoeld om uitvoering te geven aan de door de Veiligheidsraad op grond van Hoofdstuk VII van het Handvest van de Verenigde Naties aangenomen resoluties, wordt getoetst door de gerechten van de Europese Unie (hoofdstuk VII heeft betrekking op het optreden met betrekking tot bedreiging van de vrede, verbreking van de vrede en daden van agressie).
[68] Artikel 13 van het EVRM verplicht lidstaten ertoe om te waarborgen dat "[e]enieder wiens rechten en vrijheden [...] zijn geschonden, recht heeft op een daadwerkelijk rechtsmiddel voor een nationale instantie". Dit hoeft niet per se een rechterlijke instantie te zijn, zoals het EHRM heeft verklaard in de punten 56 en 67 van het arrest Klass.

zijn van de autoriteiten die het toezicht uitoefenen, en voldoende macht en bevoegdheden moet krijgen om een doeltreffende en permanente controle te kunnen uitoefenen"[69].

In het Kennedy-arrest en het Klass-arrest heeft het EHRM inzicht verschaft in wat deze verwachtingen zouden kunnen inhouden in de context van geheim toezicht, wanneer de betrokkene niet in kennis wordt gesteld van de verwerking van zijn of haar gegevens. In deze beide arresten werden de instanties door het EHRM beschouwd als onafhankelijk, in het bijzonder onafhankelijk van de organen die het toezicht uitoefenen, maar ook onafhankelijk van instructies[70] van andere instanties. Meer in het bijzonder gaf het Hof in het Kennedy-arrest zijn goedkeuring aan een onafhankelijke en onpartijdige instantie die haar eigen reglement van orde had aangenomen en bestond uit leden die een hoog rechterlijk ambt bekleedden of hadden bekleed of ervaren advocaten waren[71].

Bij het uitvoeren van het onderzoek van klachten van natuurlijke personen hadden de instanties in beide arresten bovendien toegang tot alle relevante informatie, inclusief geheim materiaal. Beide beschikten ten slotte over de bevoegdheden om niet-naleving te verhelpen.[72]

Naast de vraag of de ombudsman kan worden beschouwd als een "gerecht", houdt de toepassing van artikel 47, lid 2, van het Handvest een bijkomend probleem in, omdat het stelt dat het gerecht "bij wet" moet zijn "ingesteld". Het is echter twijfelachtig of een memorandum dat de werking van een nieuw mechanisme beschrijft, als "wet" kan worden beschouwd.

Dientengevolge besloot de werkgroep - het beginsel van essentiële gelijkwaardigheid indachtig - om niet zozeer te beoordelen of een ombudsman formeel als een bij wet ingesteld gerecht kan worden beschouwd, als wel verder de nuances van de jurisprudentie uit te werken met betrekking tot de specifieke voorwaarden waaronder "rechtsmiddelen" en "verhaalsrecht" in overeenstemming met de grondrechten van de artikelen 7, 8 en 47 van het Handvest en artikel 8 (en 13) EVRM kunnen worden beschouwd. In haar verdere analyse zal de werkgroep zich, bij de bespreking van het toepassingsgebied van het nieuwe mechanisme, dus concentreren op de volgende criteria: de voorgeschreven indiening van een verzoek bij de ombudsman en ontvangst van een antwoord ("locus standi"), de onafhankelijkheid van de ombudsman, diens bevoegdheid om in het kader van zijn onderzoek toegang te krijgen tot de noodzakelijke bescheiden, waaronder geheime documenten, en om hulp te vragen van andere instanties, en ten slotte, zijn bevoegdheid om niet-naleving te verhelpen.

3.5.3.4 Het toepassingsgebied van het ombudsmanmechanisme

Met betrekking tot toegang tot het ombudsmanmechanisme is WP29 van mening dat alle personen die onderworpen zijn aan EU-recht moeten worden beschermd door de waarborgen uit hoofde van het privacyschild. Het zou niet aanvaardbaar zijn om een onderscheid te maken gebaseerd op nationaliteit, in het bijzonder aangezien de grondrechten in de EU op iedereen

69 Arrest Klass, punten 56 en 67.
[70] EHRM, arrest Klass, punten 21 en 53.
[71] De G10-commissie bestond (ten tijde van het arrest) uit drie leden, van wie de voorzitter bevoegd moet zijn om een rechterlijk ambt te bekleden, arrest Klass punten 21 en 53)
[72] EHRM, arrest Kennedy, punt 167; Arrest Klass, punten 21 en 53.

van toepassing zijn, en niet alleen op degenen die een EU-paspoort hebben. In bijlage III wordt verwezen naar "EU-burgers" zonder nader te definiëren wat daaronder wordt verstaan. De werkgroep betreurt deze onzekerheid en stelt voor opheldering te verschaffen in die zin dat alle personen die aan EU-recht onderworpen zijn, het recht hebben dat hun verzoek aan de ombudsman wordt behandeld volgens de voorwaarden van het memorandum. Bovendien zouden de Commissie en de VS moeten aangeven in hoeverre het privacyschild ook van toepassing zal zijn op burgers/ingezetenen van de EER-landen en Zwitserland, die in het verleden onder de veiligehavenregeling vielen.

Voorts signaleert WP29 enige onduidelijkheid met betrekking tot de werkingssfeer van het ombudsmanmechanisme. Terwijl het memorandum bepaalt dat de ombudsman belast is met de behandeling van verzoeken op het gebied van nationale veiligheid inzake gegevens die krachtens in het EU-recht beschikbare doorgifte-instrumenten vanuit de EU naar de VS zijn doorgegeven, wordt in het memorandum eveneens duidelijk gemaakt dat om een mechanisme "met betrekking tot inlichtingen uit berichtenverkeer" gaat. De laatste term wijst erop dat het alleen die gegevensdoorgiften betreft waarbij de gegevens zijn verzameld door middel van inlichtingen uit berichtenverkeer, wat leidt tot de vraag of bijvoorbeeld krachtens de FISA verzamelde gegevens worden beschouwd als "inlichtingen uit berichtenverkeer". Dat lijkt het geval te zijn met betrekking tot sectie 702, zoals uiteengezet op bladzijde 10 van de verklaring van het ODNI[73]. WP29 betreurt het echter dat het gebruik van de term "inlichtingen uit berichtenverkeer" in deze context onnodige onzekerheid veroorzaakt.

Een gevolg daarvan is ook dat, naar de werkgroep begrijpt, het ombudsmanmechanisme zich niet uitstrekt tot verzoeken met betrekking tot toegang door rechtshandhavingsinstanties.[74] Als dat zo is, blijft onduidelijk of het mechanisme op verzoeken van een aantal instanties, met name de CIA, van toepassing is.

3.5.3.5 "Locus standi" en de verzoekprocedure

Het is erg moeilijk om bij de gewone rechter in de Verenigde Staten een gerechtelijke procedure aan te spannen inzake toezichtsmaatregelen van de Amerikaanse overheid. De werkgroep is ervan op de hoogte dat het Hooggerechtshof heeft geoordeeld dat locus standi in zaken betreffende inlichtingen ontbrak wanneer de verzoeker niet kon aantonen dat er sprake was van "concrete, gespecificeerde, en feitelijke of dreigende schade".[75] In dit opzicht is de instelling van de ombudsman een belangrijke stap, omdat het een vorm van verhaalsrecht mogelijk maakt die anders niet zou bestaan. De werkgroep is daarom verheugd over de verduidelijking in punt 3, onder c). Op grond van dit punt hoeft voor het indienen van een verzoek in het kader van het nieuwe mechanisme niet te worden aangetoond dat feitelijk toegang tot de gegevens van de verzoeker is verkregen via activiteiten op het gebied van inlichtingen uit berichtenverkeer.

[73] Bijlage VI bij het Privacyschild, blz. 10
[74] Memorandum inzake de instelling van een ombudsman, blz. 1
[75] Clapper tegen Amnesty International USA, 568 VS ___ (2013) I, blz. 10

De werkgroep onderschrijft grotendeels de procedure voor identificatie van de klager in het kader van het ombudsmanmechanisme. Het is volstrekt logisch dat de identificatie plaatsvindt op het grondgebied van de EU, net zoals dat het geval is bij het toegangsmechanisme uit hoofde van de TFTP2-overeenkomst tussen de EU en de VS. De werkgroep kan echter niet begrijpen waarom de controle in de EU zou moeten worden uitgevoerd door de "autoriteiten in de lidstaten die bevoegd zijn voor het toezicht op de nationale veiligheidsdiensten". Op de eerste plaats lijkt het onwaarschijnlijk dat het ingevolge artikel 4, lid 2, van het Verdrag betreffende de Europese Unie, aan de Europese Commissie zou zijn om aan deze autoriteiten taken toe te kennen die duidelijk onder de bevoegdheid van de lidstaten vallen.

Gezien de verscheidenheid aan toezichsmechanismen van nationale veiligheidsdiensten in lidstaten, kan de betrokkenheid van de betrokken autoriteiten de doeltreffendheid van het systeem voor burgers in lidstaten bovendien aanzienlijk beïnvloeden. Bijvoorbeeld, in gevallen waarin verscheidene autoriteiten verantwoordelijk zijn voor het toezicht op de nationale veiligheidsdiensten en het voor het individu moeilijk kan zijn om vast te stellen wat de relevante autoriteit is, wanneer de toepasselijke nationale juridische voorschriften niet voorzien in de mogelijkheid dat personen in contact kunnen komen met het relevante toezichthoudende orgaan of wanneer deze autoriteiten niet zodanig zijn gevestigd dat ze geschikt zijn om de taken uit te voeren die in het ontwerp-adequaatheidsbesluit aan hen zijn opgedragen[76]. Gezien de betrokkenheid van gegevensbeschermingautoriteiten bij de toepassing van en het toezicht op het privacyschild, alsmede hun vergelijkbare in het kader van de TFTP2-overeenkomst, is het zinvoller om deze taak op te dragen aan de nationale gegevensbeschermingautoriteiten van de lidstaten. De werkgroep onderstreept dat zij het onwaarschijnlijk vindt dat geheime informatie zou worden verwerkt als onderdeel van een procedure voor de ombudsman van het privacyschild, aangezien elk antwoord alleen maar zal luiden "naleving" of "niet-naleving, maar verholpen".

3.5.3.6 Onafhankelijkheid

De verklaringen van de minister van Buitenlandse Zaken (Secretary of State) maken duidelijk dat de rol van ombudsman zal worden vervuld door een staatssecretaris van het Amerikaanse Ministerie van Buitenlandse Zaken (Under Secretary of State of the Department of State). Hij wordt aangesteld door de president en deze benoeming vereist goedkeuring door de Senaat. Voor de rol van ombudsman is geen verdere goedkeuring vereist; de toewijzing van de rol is voldoende. De staatssecretaris wordt benoemd door de Amerikaanse president, als ombudsman geïnstrueerd door de Minister van Buitenlandse Zaken, en als staatssecretaris goedgekeurd door de Amerikaanse Senaat. Zoals de brief en de memorandumverklaringen benadrukken, is de ombudsman onafhankelijk van de Amerikaanse inlichtingengemeenschap. WP29 betwijfelt echter of de rol van ombudsman in het leven wordt geroepen binnen het meest geschikte ministerie. Enige kennis en begrip van het functioneren van de inlichtingengemeenschap lijkt vereist te zijn teneinde de taak van ombudsman doeltreffend te

[76] In sommige EU-lidstaten kunnen personen bijvoorbeeld alleen via een verzoek aan een hoog rechtscollege toegang krijgen tot informatie die in het bezit is van de nationale veiligheidsdiensten.

kunnen vervullen, terwijl tegelijkertijd inderdaad voldoende afstand van de inlichtingengemeenschap is vereist om onafhankelijk te kunnen optreden.

Het privacyschild omvat geen specifieke criteria voor het ontslag van de ombudsman. De werkgroep is derhalve van mening dat de ombudsman kan worden ontslagen uit zijn functie van ombudsman zoals hij ook kan worden ontslagen uit zijn functie van staatssecretaris van het Ministerie van Buitenlandse Zaken, wat de onafhankelijke positie van de ombudsman mogelijk kan ondermijnen.

Op het eerste gezicht is het aanstellen van een staatssecretaris van het Ministerie van Buitenlandse Zaken als ombudsman in termen van onafhankelijkheid duidelijk iets anders dan het vaststellen van de jurisdictie van een gewone rechtbank voor het verhaalsrecht van een individu. De vraag is dus of de ombudsman, in termen van onafhankelijkheid, kan worden beschouwd als gelijk aan andere onafhankelijke toezichtorganen die aan de vereisten voldoen. In de context van toezicht zijn dat in het bijzonder het Investigatory Powers Tribunal (IPT) in het VK en de G10-Kommission in Duitsland.

Of dit het geval is, moet apart worden beoordeeld door het analyseren van de aan de "onafhankelijke" functionaris verleende bevoegdheden.

3.5.3.7 Onderzoeksbevoegdheden

In het Kadi II-arrest heeft het HvJEU bepaald dat artikel 47 Handvest vereist dat "de belanghebbende kennis kan nemen van de gronden waarop het tegen hem genomen besluit is gebaseerd, hetzij door lezing van het besluit zelf, hetzij doordat de redenen hem op zijn verzoek worden meegedeeld, onverminderd het recht van de bevoegde rechter om te eisen dat de betrokken autoriteit hem die redenen meedeelt, teneinde hem de mogelijkheid te bieden zijn rechten onder zo goed mogelijke omstandigheden te verdedigen".[77] De rechtbanken van de Europese Unie moeten zich ervan vergewissen dat dat besluit berust op een voldoende solide feitelijke grondslag[78]. Het geeft duidelijk aan dat "de geheimhouding of de vertrouwelijkheid van die informatie of dat bewijs niet kan worden tegengeworpen", althans niet aan de Unierechter[79]. Daarom concludeert de werkgroep dat, om aan de eisen van het HvJEU te voldoen, aan de ombudsman de informatie en het bewijs moeten worden voorgelegd op grond waarvan een maatregel wordt opgelegd[80].

Het is nog onduidelijk hoever de onderzoeksbevoegdheden van de ombudsman zouden reiken. Noch het ontwerpbesluit van de Commissie noch bijlage III van het Amerikaanse Ministerie van Buitenlandse Zaken is bijzonder duidelijk over deze kwestie. Naar de werkgroep begrijpt, moet de ombudsman voldoende informatie krijgen om te kunnen verklaren of een gegevensverwerkingsoperatie door de veiligheidsdiensten in overeenstemming met de wet plaatsvindt, en om – zo dit niet het geval is – ervoor te zorgen

[77] Arrest Kadi II, punt 100.
78 Arrest Kadi II, punt 119.
79 Arrest Kadi II, punt 125.
[80] Arrest Kadi II, punt 122; hoewel de betrokken instantie niet alle informatie en al het bewijs hoeft te leveren op grond waarvan een maatregel wordt genomen.

dat deze situatie wordt rechtgezet. Noch de brief van het Ministerie van Buitenlandse Zaken noch het ontwerpbesluit specificeert echter of de ombudsman rechtstreeks toegang zou hebben tot de gegevens die over de persoon in kwestie worden bewaard en dus zijn eigen onderzoek kan uitvoeren, of dat hij is aangewezen op de verslagen van andere Amerikaanse regeringsfunctionarissen.

3.5.3.8 Corrigerende bevoegdheden

Het blijft tamelijk onduidelijk in het memorandum op welke manier de ombudsman opdracht kan geven om niet-naleving te verhelpen. Mede gelet op het gebrek aan duidelijkheid over de onderzoeksbevoegdheden blijft bovendien onduidelijk in hoeverre de ombudsman als zodanig effectief in staat zal zijn om opdracht te geven om niet-naleving te verhelpen en wat het resultaat van een dergelijke toedracht zou zijn. Zou dit kunnen betekenen dat gegevens die op een niet-conforme wijze (d.w.z. onrechtmatig) zijn verkregen niet langer kunnen worden gebruikt in een procedure en gewist moeten worden?

Verder begrijpt de werkgroep dat het privacyschild niet voorziet in een rechtsmiddel tegen of toetsing van het "besluit" van de ombudsman.

Tot slot, waar het gaat om de communicatie tussen de ombudsman en de klager na het onderzoek door de ombudsman van de klacht, mag de ombudsman niet bekend maken of de inlichtingendiensten zich onrechtmatig hebben gedragen. Het gegeven antwoord zal altijd hetzelfde en niet-specifiek zijn. In het Kadi II-arrest heeft het HvJEU verklaard dat de bevoegde autoriteit (als een controleorgaan) verplicht is om redenen aan te geven die alle omstandigheden in aanmerking nemen, hoewel artikel 296 VWEU geen gedetailleerd antwoord vereist[81].

3.5.4 Conclusie

Het bestaan van doeltreffende rechtsmiddelen voor natuurlijke personen blijft een punt van zorg voor WP29. Op de eerste plaats geeft het ontwerp-adequaatheidsbesluit geen duidelijk antwoord op de vraag in welke situaties en onder welke randvoorwaarden natuurlijke personen een zaak kunnen inleiden tot vaststelling van hun rechten.

WP29 erkent en verwelkomt de introductie van een alternatief verhaalsmechanisme in de vorm van de ombudsman, wat een unieke ontwikkeling is in de betrekkingen tussen de EU en een derde land. Afgezien van de noodzaak om de term "EU-burgers" te verduidelijken zoals eerder vermeld, creëert het mechanisme voor hen een extra beroepsgang jegens de Amerikaanse overheid teneinde te waarborgen dat alle persoonsgegevens van de verzoeker in overeenstemming met het Amerikaanse recht worden verwerkt.

Tegelijkertijd stelt WP29 aanzienlijke onvolkomenheden vast naar aanleiding van haar beoordeling van het ombudsmanmechanisme aan de hand van de normen voor een onafhankelijk gerecht in de zin van artikel 47 Handvest en de eisen die het HvJEU en het

[81] Arrest Kadi II, punt 116.

EHRM in hun jurisprudentie in toezichtszaken hebben vastgesteld. Op de eerste plaats bestaan er zorgen of de ombudsman wel (formeel en volledig) onafhankelijk kan worden geacht, in het bijzonder vanwege het relatieve gemak waarmee politiek benoemde personen kunnen worden ontslagen. Op de tweede plaats blijven er zorgen met betrekking tot de bevoegdheden van de ombudsman om doeltreffende en permanente controle uit te oefenen. Op basis van de beschikbare informatie in bijlage III kan WP29 niet tot de conclusie komen dat de ombudsman te allen tijde rechtstreeks toegang zal hebben tot alle informatie, bestanden en IT-systemen die nodig zijn om zijn eigen beoordeling te maken, en ook niet tot de conclusie komen dat hij de verantwoordelijke inlichtingendiensten daadwerkelijk kan dwingen om een einde te maken aan niet-conforme gegevensverwerking, zeker in het geval van onenigheid over de vraag of de gegevensverwerking in overeenstemming is met de wet. Mogelijk kan verdere verduidelijking van de positie en bevoegdheden van de ombudsman de zorgen van WP29 wegnemen.

3.6 Slotopmerkingen over waarborgen en beperkingen die van toepassing zijn op nationale veiligheidsautoriteiten in de VS

Op de eerste plaats prijst WP29 de Commissie en de Amerikaanse regering om alle inspanningen die zijn verricht om de gevolgen inzichtelijker te maken die Amerikaanse toezichtsprogramma's kunnen hebben voor overeenkomstig het privacyschild - of elk ander doorgifte-instrument wat dat betreft - doorgegeven gegevens. Sinds de eerste onthullingen door Snowden in juni 2013 zijn belangrijke maatregelen genomen. Toch blijven er volgens WP29 zorgen bestaan. Er zijn op zijn allerminst aanvullende verklaringen en verduidelijkingen nodig inzake de rechten en plichten overeenkomstig het privacyschild.

De twee belangrijkste zorgen van WP29 betreffen het feit dat het grootschalig en ongedifferentieerd verzamelen van gegevens niet volledig wordt uitgesloten door de Amerikaanse autoriteiten en dat de bevoegdheden en positie van de ombudsman niet gedetailleerder zijn beschreven. Bovendien zouden de nationale gegevensbeschermingsautoriteiten in plaats van de organen voor toezicht op de inlichtingendiensten bevoegd moeten zijn om namens een natuurlijk persoon een procedure in gang te zetten voor de ombudsman. Hoewel WP29 de pogingen om tegemoet te komen aan de door de gegevensbeschermingsautoriteiten geformuleerde zorgen beslist op hun waarde weet te schatten, zouden daarnaast verdere waarborgen worden toegejuicht die ervoor zorgen dat de Amerikaanse toezichtprogramma's alleen tot inmenging leiden die in een democratische samenleving noodzakelijk is.

4. BEOORDELING VAN DE DOOR HET PRIVACYSCHILD GEBODEN GARANTIES INZAKE RECHTSHANDHAVING

4.1 Inleiding

Met betrekking tot openbare toegang tot persoonsgegevens voor rechtshandhavingsdoeleinden merkt WP29 op dat de privacybeginselen in bijlage II bij het privacyschild een afwijking bevatten die identiek is aan de afwijking die was neergelegd in de privacybeginselen van de

veilige haven. De algemene aard van de afwijking is dus in stand gehouden, wat betekent dat de nieuwe privacyschildbeginselen inmenging mogelijk maken in de grondrechten van de personen wier persoonsgegevens worden doorgegeven vanuit de EU naar de VS "op grond van de eisen van de nationale veiligheid en het algemeen belang of de nationale wetgeving van de Verenigde Staten"[82].

Een van de belangrijkste punten van kritiek die het Hof in Schrems tegen de Veiligehavenbeschikking heeft ingebracht, was echter dat het "geen enkele vaststelling [bevat] ten aanzien van de vraag of er in de Verenigde Staten overheidsregels bestaan ter beperking van dergelijke inmengingen in de grondrechten van de personen van wie de gegevens vanuit de Unie naar de Verenigde Staten worden doorgegeven".

WP29 verwelkomt daarom de inspanning van de Amerikaanse regering om meer inzicht te verschaffen in het juridische kader inzake de inmenging in persoonsgegevens die overeenkomstig het privacyschild zijn doorgegeven voor rechtshandhavingsdoelstellingen, met inbegrip van de toepasselijke beperkingen en waarborgen. Tegelijkertijd benadrukt WP29 dat zij de kwestie van openbare toegang beziet in het licht van het feit dat elke inmenging in de grondrechten op privéleven en gegevensbescherming gerechtvaardigd moet zijn in een democratische maatschappij. WP29 heeft daarom de waarborgen op het gebied van rechtshandhaving van het privacyschild geanalyseerd en daarbij gebruik gemaakt van het kader dat in punt 1.2 van dit advies is beschreven.

4.2. Toepassing van de Europese essentiële waarborgen op toegang door rechtshandhavingsautoriteiten tot gegevens in het bezit van ondernemingen

4.2.1 Toegang door rechtshandhavingsautoriteiten tot persoonsgegevens moet in overeenstemming zijn met de wet en gebaseerd zijn op duidelijke, nauwkeurige en toegankelijke voorschriften

Bijlage VII bij het privacyschild bevat een brief van het Amerikaanse Ministerie van Justitie "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".

Alle in bijlage VII genoemde procedures vloeien ofwel rechtstreeks voort uit de Amerikaanse Grondwet (het Vierde amendement), ofwel voort uit geschreven wetten en procesrecht of richtlijnen en beleid van het Amerikaanse Ministerie van Justitie. Bijlage VII verwijst echter niet specifiek naar alle wetten waarbij deze procedures zijn vastgesteld, maar beperkt zich in plaats daarvan tot een beknopte beschrijving van de procedures zelf. Bijlage VII vermeldt ook 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

[82] Arrest Schrems, punt 87

gegevens die zij verwerken", en geeft een niet-limitatief aantal voorbeelden zoals de Bank Secrecy Act, de Fair Credit Reporting Act en de Right to Financial Privacy Act.

WP29 merkt op dat het kader van wetten, procedures en beleid versnipperd is en dat de toepasselijke rechtsgrondslag voor een bepaald verzoek om toegang afhankelijk zal zijn van de aard van de gevraagde gegevens, de aard van het bedrijf, de aard van de juridische procedures (strafrechtelijk, administratief, verbonden met ander algemeen belang) en de aard van de entiteit die om toegang verzoekt.

Aangezien alle toepasselijke voorschriften om de toegang van wetshandhavingsautoriteiten te beperken tot volgens het privacyschild doorgegeven gegevens, zijn gebaseerd op de Grondwet, op geschreven recht en op transparant beleid van het Ministerie van Justitie, gaat WP29 uit van de veronderstelling dat deze voorschriften toegankelijk zijn. De duidelijkheid en nauwkeurigheid van de voorschriften kan echter alleen worden beoordeeld ten aanzien van elk specifiek soort procedure en verzoek om toegang. WP29 betreurt het daarom dat, uitgaande van de beschikbare gegevens in bijlage VII bij het privacyschild en de bevindingen in het ontwerpbesluit, een dergelijke beoordeling op dit moment niet kan worden uitgevoerd.

4.2.2 Noodzakelijkheid en evenredigheid met betrekking tot de legitieme doelstellingen moeten worden aangetoond

WP29 merkt op dat het verzoek om toegang tot gegevens voor rechtshandhavingsdoeleinden kan worden beschouwd als het nastreven van een legitieme doelstelling. Artikel 8, lid 2, EVRM laat bijvoorbeeld inmenging toe in het recht op de bescherming van het privéleven door enig openbaar gezag "in het belang van [...] de openbare veiligheid, [of] het voorkomen van wanordelijkheden of strafbare feiten". Een dergelijke inmenging is echter alleen acceptabel als deze noodzakelijk en evenredig is[83].

Volgens de vaste rechtspraak van het HvJEU vereist het evenredigheidsbeginsel dat de wetgevende maatregelen die inmenging mogelijk maken in de rechten op privéleven en de bescherming van persoonsgegevens "geschikt zijn om de door *de betrokken regeling* nagestreefde legitieme doelstellingen te verwezenlijken en niet verder gaan dan wat daarvoor geschikt en noodzakelijk is"[84] (cursivering door ons aangebracht). Daarom wordt de beoordeling van noodzakelijkheid en evenredigheid altijd uitgevoerd met betrekking tot een specifieke door de wetgeving beoogde maatregel.

De Amerikaanse autoriteiten geven in bijlage VII nader aan dat federale aanklagers en federale onderzoeksagenten toegang kunnen krijgen tot documenten en andere gegevens van bedrijven door middel van "meerdere soorten dwingende rechtsfiguren, waaronder dagvaardingen van de kamer van inbeschuldigingstelling, administratieve dwangbevelen en huiszoekingsbevelen" en andere communicatie kunnen verkrijgen "op grond van federale

[83] Zie het werkdocument inzake de Europese essentiële waarborgen, blz 7-9. Zie voor een algemene beoordeling van de begrippen noodzakelijkheid en evenredigheid, WP29 "Advies 01/2014 over de toepassing van noodzakelijkheids- en evenredigheidsconcepten en gegevensbescherming binnen de wethandhavingssector", 27 februari 2014.
[84] Arrest Digital Rights Ireland, punt 46 en de daar aangehaalde rechtspraak.

bevoegdheden voor afluisteren en nummerregistratie"[85]. Bovendien kunnen instanties met civiele en regelgevende verantwoordelijkheden jegens organisaties een dwangbevel uitvaardigen inzake "bedrijfsgegevens, elektronisch opgeslagen informatie of andere tastbare zaken"[86]. Bijlage VII specificeert verder dat deze juridische procedures over het algemeen worden gebruikt om informatie te verkrijgen van "ondernemingen" in de VS, ongeacht of ze binnen het kader van het privacyschild gecertificeerd zijn of niet, en "ongeacht de nationaliteit van de betrokkene". Met andere woorden, het lijkt erop dat de bescherming organisaties betreft en niet het individu als zodanig.

Naast bijlage VII bevat het ontwerpbesluit - dat is gebaseerd op de privacyschildbeginselen - bevindingen van de Commissie met betrekking tot het bestaan in de VS van voorschriften om inmenging te beperken in de grondrechten van personen wier persoonsgegevens onder het privacyschild worden doorgegeven van de EU naar de VS.

De bevindingen in het ontwerpbesluit verwijzen in het bijzonder naar toepasselijke beperkingen en waarborgen krachtens het Vierde amendement van de Amerikaanse grondwet, op grond waarvan voor huiszoekingen en inbeslagnemingen door rechtshandhavingsinstanties in beginsel een rechterlijk bevel op grond van een "redelijk vermoeden" vereist is[87]. De bevindingen verwijzen ook naar het feit dat in de uitzonderlijke gevallen waarin geen bevel vereist is, de rechtshandhaving onderworpen is aan een redelijkheidstoets[88].

De bevindingen maken echter niet duidelijk op welke wijze deze waarborgen van toepassing zijn op niet-Amerikanen. In feite erkent het ontwerpbesluit in een overweging dat "de bescherming volgens het vierde amendement zich niet uitstrekt tot niet-Amerikanen die niet in de Verenigde Staten woonachtig zijn"[89]. In hetzelfde punt van het ontwerpbesluit wordt verder bepaald dat niet-Amerikanen "indirect profiteren van de bescherming die wordt verleend aan Amerikaanse ondernemingen die de persoonsgegevens in handen hebben en die de ontvangers van rechtshandhavingsverzoeken zijn". WP29 betreurt het echter dat deze bevinding niet verwijst naar een juridische bron, hetzij in het geschreven recht hetzij in de jurisprudentie.

Al met al merkt WP29 op dat het systeem van 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 - met inbegrip van de toegangsbeperkingen en waarborgen - een complex geheel van maatregelen is. Dit systeem kan op dit moment op basis van de beschikbare informatie niet in zijn algemeenheid worden beoordeeld. Specifieke beoordeling in individuele gevallen is nodig om echt te kunnen beoordelen of de onderzoeksmaatregelen op het gebied van rechtshandhaving noodzakelijk en evenredig zijn met betrekking tot de grondrechten betreffende het privéleven en gegevensbescherming.

[85] Bijlage VII, blz. 2.
[86] Bijlage VII, blz. 4.
[87] Ontwerp-adequaatheidsbesluit, punt107
[88] Privacyschild, punt 107
[89] Ontwerp-adequaatheidsbesluit, punt 108

4.2.3 Er moet een onafhankelijk toezichtsmechanisme voorhanden zijn

WP29 neemt nota van het feit dat de meeste in bijlage VII beschreven procedures veronderstellen dat voordat autoriteiten toegang krijgen tot gegevens er eerst sprake van een besluit van een gerecht moet zijn (bijv. gerechtelijke bevelen voor nummerregistratie en traceerapparatuur, gerechtelijke bevelen voor surveillance op grond van de federale wetgeving inzake afluisteren, huiszoekingsbevelen - regel 41). Het lijkt er echter op dat ze niet allemaal voorafgaande betrokkenheid van een gerecht vereisen. Civiele en regelgevende instanties bijvoorbeeld "kunnen een dagvaarding uitbrengen"[90]. In deze gevallen is er de mogelijkheid van een ex post rechterlijke controle van de redelijkheid van de dagvaarding, aangezien "een ontvanger van een administratief dwangbevel de handhaving van dat dwangbevel [kan] aanvechten voor de rechter"[91].

Uitgaande van de beschikbare informatie merkt WP29 op dat er - met betrekking tot toegang door rechtshandhavingsautoriteiten tot gegevens die in het bezit zijn van bedrijven in de VS - een tamelijk solide en onafhankelijk toezichtmechanisme aanwezig lijkt te zijn.

4.2.4 Individuen moeten de beschikking over doeltreffende rechtsmiddelen hebben

Zoals hiervoor genoemd, "strekt de bescherming van het vierde amendement zich niet uit tot niet-Amerikanen die niet in de Verenigde Staten wonen"[92]. Dit betekent dat een niet-Amerikaan voor de rechter geen bevelen of dwangbevelen zou kunnen aanvechten op basis van het vierde amendement. Het ontwerp-adequaatheidsbesluit specificeert dat niet-Amerikanen indirect profiteren van de bescherming die wordt verleend aan Amerikaanse ondernemingen die de persoonsgegevens in handen hebben en die de ontvangers van rechtshandhavingsverzoeken zijn. WP29 merkt echter op dat, zelfs als deze bescherming doeltreffend zou zijn, dit niet betekent dat natuurlijke personen de beschikking over doeltreffende rechtsmiddelen hebben, aangezien het voorwerp van het recht op een doeltreffend rechtsmiddel in dit scenario de onderneming lijkt te zijn die het verzoek om toegang ontvangt, en niet de natuurlijke persoon om wiens gegevens het gaat.

Bijlage VII bevat geen verdere informatie over mogelijke rechtsmiddelen op basis van de geschreven wetgeving die niet-Amerikanen ter beschikking staan wanneer autoriteiten of ondernemingen onrechtmatig toegang verschaffen of verkrijgen tot de inhoud van hun gegevens.

WP29 verwelkomt het feit dat de onlangs aangenomen Judicial Redress Act[93] aan niet-Amerikanen het recht op gerechtelijk beroep verschaft. De betreffende rechten zijn echter beperkt tot duidelijk gedefinieerde gevallen: het recht om correctie en toegang tot gegevens en advocatenhonoraria te verkrijgen wanneer een "aangewezen federaal agentschap of onderdeel" rectificatie van gegevens weigert of toegang tot zulke gegevens weigert en het

[90] Bijlage VII, blz. 4.
[91] Bijlage VII, blz. 4.
[92] Ontwerp-adequaatheidsbesluit, punt 108.
[93] Judicial Redress Act van 2015, H.R. 1428.

recht op civiele rechtsmiddelen in geval van "doelbewuste of opzettelijke" openbaarmaking van gegevens.

Bovendien is de Amerikaanse jurisprudentie waarnaar wordt verwezen in de voetnoten van de relevante overwegingen van het ontwerpbesluit, in het bijzonder de arresten City of Ontario/Quon[94], Maryland/King[95] en Samson/Californië[96], niet van belang voor de beoordeling of niet-Amerikanen naar de rechter kunnen stappen om de rechtmatigheid van een inmenging in hun privéleven aan te vechten[97]. Alle arresten verwijzen naar het recht op privéleven van Amerikanen, en alle bevatten ze besluiten van het Amerikaanse Hooggerechtshof die in feite de toepassing van het Vierde amendement beperken.

Al met al erkent en verwelkomt WP29 de vaststelling van de Judicial Redress Act, maar blijft zij twijfelen of individuele betrokkenen daadwerkelijk over doeltreffende rechtsmiddelen beschikken.

4.3 Slotopmerkingen

WP29 verwelkomt en erkent de inspanning van de Amerikaanse regering om meer inzicht te verschaffen in het juridische kader inzake de inmenging in persoonsgegevens die onder het EU-VS privacyschild zijn doorgegeven voor rechtshandhavingsdoelstellingen, met inbegrip van de toepasselijke beperkingen en waarborgen.

WP29 merkt op dat het systeem van onderzoeksinstrumenten van rechtshandhavingsautoriteiten, inclusief de toepasselijke beperkingen en waarborgen, zowel veelomvattend als complex is en dat de in het privacyschild opgenomen informatie beknopt is. WP29 betreurt het daarom dat zij, gebaseerd op de beperkte informatie (d.w.z. in bijlage VII bij het privacyschild en de bevindingen in het ontwerpbesluit), op dit moment geen uitgebreide beoordeling kan geven met betrekking tot de toegankelijkheid, voorzienbaarheid en de noodzakelijkheid en evenredigheid van de toepasselijke voorschriften. Ondanks de andere bevindingen van WP29 met betrekking tot het privacyschild in dit advies, zou een dergelijke beoordeling onderdeel kunnen zijn van een jaarlijkse beoordeling van het privacyschild.

Met betrekking tot toegang door rechtshandhavingsautoriteiten merkt WP29 op dat er een tamelijk solide en onafhankelijk toezichtsmechanisme aanwezig lijkt te bestaan. Voorts verwelkomt WP29 de goedkeuring van de Judicial Redress Act, die niet-Amerikanen het

[94] *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).
[95] *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).
[96] *Samson v. California*, 547 U.S. 843, 848 (2006).
[97] In het arrest *Ontario v. Quon* heeft het Hof beslist dat de stad Ontario de rechten van zijn werknemers uit hoofde van het vierde amendement niet schond, omdat de toegang van de stad tot de inhoud van de persoonlijke berichten van de werknemer in kwestie redelijk was, aangezien deze werd gemotiveerd door een rechtmatig werkgerelateerd doel en niet buitensporig was. In het arrest *Samson/ Californië* heeft het Hof geoordeeld dat "het vierde amendement een politieagent niet verbiedt om een voorwaardelijk vrijgelatene zonder verdenking aan een onderzoek te onderwerpen". In het arrest *Maryland/ King* heeft het Hof beslist dat wanneer politieagenten op basis van een redelijk vermoeden van schuld tot arrestatie overgaan en een verdachte in verband met een ernstig misdrijf aanhouden en naar het bureau brengen om hem in hechtenis te nemen, het nemen en analysen van wangslijm-DNA van de arrestant, net als vingerafdrukken en foto's, een rechtmatige en op grond van het vierde amendement redelijke politieprocedure is.

recht geeft om naar de rechter te stappen. WP29 merkt echter op dat de betreffende rechten beperkt van aard zijn. Naast de conclusie dat een niet-Amerikaan bij het Hof niet met een beroep op het vierde amendement in beroep zou kunnen gaan tegen bevelen of dagvaarding, blijven er zorgen over bestaan of natuurlijke personen op het gebied van rechtshandhaving daadwerkelijk over doeltreffende rechtsmiddelen beschikken.

5. CONCLUSIES EN AANBEVELINGEN

WP29 is in de eerste plaats verheugd over het feit dat binnen vijf maanden na de ongeldigverklaring van de veiligehavenbeschikking, een nieuw ontwerp-adequaatheidsbesluit is gepresenteerd dat veel verbeteringen bevat ten opzichte van het vorige mechanisme. Zij is vooral ingenomen met de toegenomen transparantie als gevolg van de opneming van twee privacyschildlijsten op de website van het DoC: één lijst die de gegevens bevat van de organisaties die het privacyschild onderschrijven en één lijst die de gegevens bevat van de organisaties die in het verleden het schild hebben onderschreven, maar dit niet langer doen. Ook de toegenomen transparantie met betrekking tot de toegang van het publiek tot gegevens die, hetzij ten behoeve van de nationale veiligheid hetzij ten behoeve van rechtshandhaving, onder het privacyschild zijn doorgegeven, wordt toegejuicht. Tot slot is WP29 zeer tevreden om te vernemen dat alle doorgiften van gegevens naar de VS voortaan dezelfde bescherming zullen genieten: er zijn geen specifieke wettelijke bepalingen van kracht die aan een bepaald instrument de voorkeur geven boven een ander.

5.1 Drie punten van zorg

Er blijven echter drie belangrijke punten van zorg bestaan, die volgens WP29 tot maatregelen nopen.

Het eerste betreft het feit dat de in het ontwerp-adequaatheidsbesluit gebruikte bewoordingen organisaties er niet toe verplichten om gegevens die niet langer nodig zijn, te wissen. Dit is een essentieel element van EU-wetgeving inzake gegevensbescherming dat waarborgt dat gegevens niet langer worden bewaard dan nodig is om het doel waarvoor de gegevens zijn verzameld, te bereiken. Op de tweede plaats maakt WP29 uit bijlage VI op dat de Amerikaanse regering de voortgezette grootschalige en willekeurige verzameling van gegevens niet volledig uitsluit. WP29 heeft zich steeds op het standpunt gesteld dat een dergelijke verzameling van gegevens een ongerechtvaardigde inmenging in de grondrechten van natuurlijke personen is. Het derde punt van zorg betreft de invoering van het ombudsmanmechanisme. Hoewel WP29 deze unieke stap, waarmee een extra verhaals- en toezichtsmechanisme voor natuurlijke personen wordt gecreëerd, verwelkomt, blijven zorgen bestaan of de ombudsman wel voldoende bevoegdheden heeft om doeltreffend te functioneren. Op zijn minst moeten zowel de bevoegdheden als de positie van de ombudsman worden verduidelijkt teneinde aan te tonen dat de functie werkelijk onafhankelijk is en als doeltreffend rechtsmiddel kan dienen voor niet-conforme gegevensverwerking.

5.2 Aanbevolen verduidelijkingen

Naast de bovengenoemde punten heeft WP29 in dit advies diverse punten aangestipt waar verdere verduidelijking van het adequaatheidsbesluit op zijn plaats is. Daarbij gaat het eerst en vooral om de noodzaak te waarborgen dat de belangrijke begrippen inzake gegevensbescherming die in het privacyschild worden gebruikt op een consistente manier worden gedefinieerd en toegepast. Daar is op dit moment geen sprake van. De invoering van een verklarende woordenlijst bij de FAQ betreffende het privacyschild, met definities die bij voorkeur tussen de EU en de VS zijn overeengekomen, zou wenselijk zijn. WP29 concludeert ook dat verdere doorgifte van EU-persoonsgegevens onvoldoende geregeld is, vooral met betrekking tot het toepassingsgebied, de doelbinding en de garanties die van toepassing zijn op doorgiften aan vertegenwoordigers. Wat de toegang betreft tot privacyschildgegevens ten behoeve van rechtshandhaving, baart vooral de voorspelbaarheid van de wetgeving zorgen, vanwege de uitvoerige en complexe aard van het Amerikaanse rechtshandhavingssysteem op zowel federaal als nationaal niveau, en de beperkte informatie die in het adequaatheidsbesluit is opgenomen.

Het privacyschild is het eerste adequaatheidsbesluit dat is opgesteld sinds over de tekst van de algemene verordening gegevensbescherming in principe overeenstemming werd bereikt. Toch komen veel verbeteringen op het niveau van gegevensbescherming voor natuurlijke personen in het privacyschild niet tot uitdrukking. WP29 adviseert daarom om kort na de inwerkingtreding van de algemene verordening gegevensbescherming dit adequaatheidsbesluit, alsook de voor andere derde landen uitgevaardigde adequaatheidsbesluiten te evalueren.

Een laatste aanbeveling van WP29 die hier benadrukt moet worden, betreft de gezamenlijke evaluatie. WP29 verwelkomt het feit dat het adequaatheidsbesluit van het privacyschild elk jaar zal worden geëvalueerd, met een brede betrokkenheid van autoriteiten voor gegevensbescherming en andere relevante partijen. Zij zou overeenstemming over de elementen van de gezamenlijke evaluaties toejuichen, inclusief de opstelling en presentatie van het evaluatieverslag door alle partijen ruim vóór de eerste evaluatie.