EUROPESE
COMMISSIE

Brussel, 9.10.2024
COM(2024) 451 final

VERSLAG VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

over de eerste periodieke evaluatie van de werking van het adequaatheidsbesluit inzake het kader voor gegevensbescherming EU-VS

1. DE EERSTE EVALUATIE — ACHTERGROND, VOORBEREIDING EN PROCES

In haar besluit van 10 juli 2023 (het "adequaatheidsbesluit") heeft de Commissie vastgesteld dat het EU-VS-kader voor gegevensbescherming (EU-VS-Data Privacy Framework, hierna "DPF" genoemd) een passend beschermingsniveau biedt voor persoonsgegevens die vanuit de Europese Unie worden doorgegeven aan organisaties in de Verenigde Staten (VS)[1]. Het adequaatheidsbesluit vereist dat de Commissie periodieke evaluaties verricht, waarvan de eerste een jaar na de datum van kennisgeving van het adequaatheidsbesluit aan de lidstaten moet plaatsvinden. Met dit verslag wordt de eerste evaluatie afgesloten.

Overeenkomstig overweging 211 van het adequaatheidsbesluit ligt de focus van deze eerste evaluatie, die is uitgevoerd na het eerste jaar van werking van het nieuwe kader, op de vraag of alle relevante elementen waarin het kader voorziet, volledig zijn uitgevoerd en in de praktijk effectief functioneren. De evaluatie bestrijkt alle aspecten van de werking van het kader, ook in het licht van de wettelijke ontwikkelingen die zich hebben voorgedaan sinds de vaststelling van het adequaatheidsbesluit.

Ter voorbereiding van de evaluatie heeft de Commissie informatie verzameld van belanghebbenden, met name van niet-gouvernementele organisaties (ngo's) met deskundigheid op het gebied van digitale rechten en gegevensbescherming[2] en DPF-gecertificeerde organisaties (via hun brancheorganisaties[3]), alsmede van de Amerikaanse autoriteiten die betrokken zijn bij de uitvoering van het kader. Daarnaast heeft de Commissie feedback van het algemene publiek verkregen door middel van een specifiek verzoek om input op het "Geef uw mening"-portaal[4].

Op 18 en 19 juli 2024 is een evaluatievergadering gehouden in Washington D.C. De vergadering werd geopend door EU-commissaris voor Justitie en Consumentenzaken Didier Reynders en de Amerikaanse minister van Handel Gina Raimondo[5].

---

[1] Uitvoeringsbesluit EU 2023/1795 van de Europese Commissie van 10 juli 2023 uit hoofde van Verordening (EU) 2016/679 van het Europees Parlement en de Raad inzake het passende niveau van bescherming van persoonsgegevens krachtens het EU-VS-kader voor gegevensbescherming.

[2] De Commissie heeft een vragenlijst toegezonden aan negen ngo's (Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center, Center for Democracy and Technology), waarin de nadruk lag op relevante ontwikkelingen in het rechtskader, de toezichts- en handhavingsmechanismen en de werking van verhaalsmechanismen van de VS. Ook hebben de diensten van de Commissie en vertegenwoordigers van het Europees Comité voor gegevensbescherming (EDPB) op 9 juli 2024 online met deze ngo's vergaderd.

[3] De Commissie heeft een vragenlijst toegezonden aan negen brancheorganisaties (Software & Information Industry Association, U.S. Chamber of Commerce, Information Technology Industry Council, the Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association, Engine), waarin de nadruk lag op de ervaringen van DPF-gecertificeerde bedrijven, met name het certificeringsproces, de stappen die zijn gezet om de DPF-beginselen na te leven, mechanismen voor de behandeling van verzoeken en klachten van betrokkenen enz.

[4] De ontvangen feedback is te vinden via de volgende link: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-EU-US-Data-Privacy-Framework-report-of-the-Commission-on-how-the-framework-is-functioning_nl.

[5] De evaluatievergadering was onderverdeeld in agendapunten, waarbij elk specifiek agendapunt werd ingeleid middels een korte presentatie door de desbetreffende Amerikaanse autoriteit, EU-vertegenwoordiger of organisatie, gevolgd door een uitgebreide vraag-en-antwoordsessie. De "commerciële aspecten" van het kader (d.w.z. de toepassing en handhaving van de vereisten voor DPF-gecertificeerde bedrijven) werden op de eerste

Voor de EU werd de evaluatie uitgevoerd door vertegenwoordigers van het directoraat-generaal Justitie en Consumentenzaken van de Europese Commissie, samen met vijf door de EDPB aangewezen vertegenwoordigers van verschillende nationale gegevensbeschermingsautoriteiten en de Europese Toezichthouder voor gegevensbescherming (EDPS)[6]. Van Amerikaanse zijde werd aan de vergadering deelgenomen door vertegenwoordigers van het ministerie van Handel (Department of Commerce), het ministerie van Buitenlandse Zaken (Department of State), de federale commissie voor de handel (Federal Trade Commission, "FTC"), het ministerie van Vervoer (Department of Transportation), het bureau van de directeur voor de nationale inlichtingendiensten (Office of the Director of National Intelligence, "ODNI"), het ministerie van Justitie (Department of Justice), de inspecteur-generaal voor de inlichtingendiensten (Inspector General for the Intelligence Community) en leden van de Raad van toezicht op de privacy en de burgerlijke vrijheden (Privacy and Civil Liberties Oversight Board, "PCLOB"). Daarnaast hebben vertegenwoordigers van organisaties die onafhankelijke geschillenbeslechtingsdiensten aanbieden en de American Arbitration Association informatie verstrekt tijdens de evaluatiesessies waaraan zij hebben deelgenomen. Bovendien is bij de evaluatie gebruikgemaakt van presentaties van DPF-gecertificeerde organisaties over de wijze waarop bedrijven de vereisten van het kader naleven.

De bevindingen van de Commissie stoelen voorts op informatie uit openbare bronnen, zoals rechterlijke beslissingen, uitvoeringsbepalingen en procedures van de desbetreffende Amerikaanse autoriteiten, verslagen en studies van ngo's, door DPF-gecertificeerde bedrijven uitgebrachte transparantieverslagen, jaarverslagen van onafhankelijke toezichthoudende instanties en mediapublicaties.

2. BEVINDINGEN

2.1. Commerciële aspecten

2.1.1. Het certificeringsproces

Om uit hoofde van het DPF vanuit de EU overgedragen persoonsgegevens te kunnen ontvangen, moet een Amerikaans bedrijf tegenover het ministerie van Handel van de VS verklaren, en dat op jaarlijkse basis opnieuw doen, dat het de specifieke vereisten voor de bescherming van gegevens (de "DPF-beginselen") in acht neemt. Voor deze certificering moet een bedrijf zijn onderworpen aan de onderzoeks- en handhavingsbevoegdheden van de FTC of het ministerie van Handel, in het openbaar verklaren dat het de verplichting aangaat om zich aan de beginselen te houden, zijn privacybeleid openbaar maken en alle vereisten volledig toepassen[7]. Voordat een certificering wordt voltooid, controleert het ministerie van Handel of het bedrijf voldoet aan alle certificeringsvereisten[8].

Tijdens de evaluatievergadering heeft het ministerie van Handel uitgelegd dat de focus in dit eerste jaar van het DPF lag op het opzetten van het certificeringsproces, dat onder meer het

dag behandeld, terwijl op de tweede dag aangelegenheden in verband met de toegang van overheidsinstanties tot persoonsgegevens werden besproken.

[6] De vertegenwoordigers van de Commissie en de EDPB zijn op 12 juni en 10 juli 2024 bijeengekomen om de evaluatie voor te bereiden, de ontvangen input te bespreken en vast te stellen welke aspecten aanvullende informatievergaring en verduidelijking behoefden.

[7] Punt I.2 van bijlage I bij het adequaatheidsbesluit.

[8] Bijlage III bij het adequaatheidsbesluit.

ontwikkelen van specifieke IT-instrumenten, het actualiseren van procedures, het aanknopen van contacten met bedrijven en het uitvoeren van andere voorlichtings-/bewustmakingsactiviteiten omvatte. Ten tijde van de evaluatievergadering waren meer dan 2 800 bedrijven DPF-gecertificeerd. Dat betekent dat meer bedrijven DPF-gecertificeerd zijn dan er gecertificeerd waren voor het vorige kader, het Privacy Shield, na het eerste jaar dat dat van kracht was[9]. Volgens informatie van het ministerie van Handel bestaat 70 % van de deelnemers uit kleine en middelgrote ondernemingen en is een groot aantal DPF-gecertificeerde bedrijven (47 %) actief in de informatie-, communicatie- en technologiesector (ICT). Voorts is 60 % van de bedrijven uitsluitend gecertificeerd voor niet-personeelsgegevens, is 2,5 % uitsluitend gecertificeerd voor personeelsgegevens en is 37,5 % gecertificeerd voor zowel personeels- als niet-personeelsgegevens.

Het ministerie van Handel heeft de benodigde procedures voor de behandeling van aanvragen van bedrijven ingevoerd. Bedrijven moeten hun aanvragen voor certificering indienen op de DPF-website van het ministerie van Handel (https://www.dataprivacyframework.gov/). Op die website wordt informatie verstrekt over hoe een bedrijf zich kan aansluiten bij het DPF[10] en over de verplichtingen van het bedrijf krachtens het kader[11]. Een specifiek team binnen het ministerie van Handel, dat rapporteert aan een speciaal voor het DPF aangestelde directeur, is verantwoordelijk voor alle aspecten van het beheer en de administratie van het DPF, waaronder het certificeringsproces en het toezicht op de naleving van het DFP. Elke aanvraag wordt toegewezen aan een bepaalde medewerker die gedurende het hele certificeringsproces verantwoordelijk blijft voor de aanvraag van het desbetreffende bedrijf.

Om DPF-gecertificeerd te kunnen worden, moeten bedrijven een aanvraag indienen die ook een ontwerp-privacybeleid omvat. Het ministerie van Handel controleert of het bedrijf voldoet aan de relevante vereisten van het DPF. Wanneer organisaties verschillende entiteiten binnen een groep van bedrijven (bv. dochterondernemingen) willen certificeren, beoordeelt het ministerie van Handel ofwel één overkoepelend privacybeleid waarin alle te certificeren entiteiten duidelijk worden vermeld, ofwel het privacybeleid van elke afzonderlijk entiteit zoals overgelegd door de organisatie. Het ministerie van Handel verifieert ook, met behulp van het in de aanvraag vermelde onafhankelijke verhaalsmechanisme[12], of de organisatie zich daadwerkelijk bij het ministerie heeft geregistreerd. Voor bedrijven die het panel van de gegevensbeschermingsautoriteit selecteren (bijvoorbeeld omdat zij personeelsgegevens verwerken), controleert het ministerie van Handel of het bedrijf de vereiste vergoedingen voor het gebruik van het panel heeft betaald. Indien nodig gaat het ministerie van Handel ook na of de aanvrager onder de jurisdictie van de FTC of van het ministerie van Vervoer valt (en derhalve in aanmerking komt voor een DPF-certificering).

Als aan alle voorwaarden is voldaan, deelt het ministerie van Handel de organisatie mee dat zij haar privacybeleid, met een verwijzing naar het DPF, op haar website kan publiceren. Zodra het privacybeleid openbaar is, bevestigt het ministerie van Handel de certificering en wordt het bedrijf opgenomen in de DPF-lijst op de website van het ministerie. Vanaf de datum waarop

[9] Na het eerste jaar van werking van het Privacy Shield waren 2 400 bedrijven gecertificeerd.
[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).
[11] https://www.dataprivacyframework.gov/key-requirements.
[12] Een geschillenbeslechtingsmechanisme in de particuliere sector waarmee individuele klachten en geschillen worden onderzocht en snel kunnen worden beslecht zonder kosten voor de betrokkene.

het ministerie van Handel de organisatie op die lijst heeft geplaatst, kunnen op basis van het DPF persoonsgegevens uit de EU worden ontvangen[13].

Zoals toegelicht tijdens de evaluatievergadering, hebben de controles die het ministerie van Handel tot nu toe heeft uitgevoerd, ertoe geleid dat 33 aanvragen zijn afgewezen omdat zij niet voldeden aan de DPF-vereisten. Het ministerie van Handel gaat doorgaans een samenwerking met het bedrijf aan om tekortkomingen te verhelpen. Wanneer het ministerie van Handel tekortkomingen vaststelt, deelt het aan het bedrijf mee dat het deze moet aanpakken en dat indien het niet binnen een gegeven tijdsbestek reageert of zijn zelfcertificering niet overeenkomstig de procedures van het ministerie voltooit, de aanvraag als geannuleerd zal worden beschouwd. Als de eerste certificering niet binnen twaalf maanden wordt voltooid/gewijzigd, beschouwt het ministerie deze als geannuleerd.

De uiterste datum voor de jaarlijkse hercertificering wordt voor elk bedrijf vermeld in de DPF-lijst. Om bedrijven eraan te herinneren dat zij om hercertificering moeten verzoeken, beschikt het ministerie over een systeem met waarschuwingen dat de certificering binnenkort zal verlopen. Een maand voor de vervaldatum, vervolgens twee weken voor de vervaldatum en daarna een dag voor de vervaldatum ontvangen organisaties een herinnering. Organisaties die hun certificering laten verlopen, worden uit de DPF-lijst verwijderd. Zoals beschreven in bijlage III bij het adequaatheidsbesluit, bevat de website van het ministerie van Handel een specifiek onderdeel met een lijst van de Amerikaanse organisaties die niet langer actieve deelnemers zijn, met vermelding van de respectieve redenen (bv. verval of intrekking) voor de verwijdering van de betrokken bedrijven uit de lijst (de "inactieve lijst"). Wanneer een organisatie van de DPF-lijst wordt geschrapt omdat zij haar certificering heeft laten verlopen, neemt het ministerie van Handel contact met haar op voor een bevestiging dat zij de certificering wil intrekken dan wel zich opnieuw wenst te certificeren, en om, in dat laatste geval, na te gaan of zij na het verlopen van de certificering de DPF-beginselen heeft toegepast op persoonsgegevens die in het kader van het DPF zijn ontvangen en welke stappen zij zal ondernemen om oplossingen te vinden voor de nog openstaande problemen die haar hercertificering hebben vertraagd. Wanneer een organisatie het ministerie laat weten dat zij zich uit het DPF wil terugtrekken, verlangt het ministerie dat zij bevestigt of zij de gegevens die zij onder het DPF heeft ontvangen, zal teruggeven of verwijderen, die gegevens zal bewaren en de DPF-beginselen op de gegevens zal blijven toepassen (hetgeen jaarlijks moet worden bevestigd), dan wel de gegevens wenst te behouden en andere beschermingsmaatregelen (zoals door de Europese Commissie vastgestelde modelcontractbepalingen) zal invoeren.

Uit feedback van brancheorganisaties en bedrijven blijkt dat DPF-gecertificeerde bedrijven een aantal stappen hebben ondernomen om de inachtneming van de DPF-beginselen te waarborgen. Om te voldoen aan het beginsel inzake verhaal, handhaving en aansprakelijkheid, hebben organisaties bijvoorbeeld interne controles uitgevoerd in de vorm van zelfbeoordelingen of externe nalevingsbeoordelingen. De twee verhaalsmechanismen in de particuliere sector waarvan vertegenwoordigers hebben deelgenomen aan de evaluatievergadering, hebben uitgelegd dat zij ook externe nalevingsbeoordelingen uitvoeren door het privacybeleid te evalueren, en de vertegenwoordiger van een van die verhaalsmechanismen lichtte toe dat er tevens audits en steekproefsgewijze controles worden uitgevoerd waarin bijvoorbeeld de beginselen van toegang, keuze en verdere doorgifte centraal staan. Daarnaast hebben gecertificeerde bedrijven interne nalevingsprogramma's en toezichtsmechanismen ontwikkeld,

[13] Punt I.3 van bijlage I bij het adequaatheidsbesluit.

werknemers opgeleid, mechanismen geïmplementeerd om betrokkenen in staat te stellen hun rechten uit te oefenen, privacyeffectbeoordelingen uitgevoerd en bestaande contracten herzien.

2.1.2. Toezicht op de naleving, valse claims van deelname en handhaving

Uit hoofde van het DPF is het ministerie van Handel van de VS verantwoordelijk voor het toezicht op de naleving van de DPF-beginselen, waartoe het beschikt over verschillende instrumenten, waaronder ambtshalve controles (controles op eigen initiatief), ad-hoccontroles ter plaatse en nalevingsvragenlijsten. Dit toezicht omvat het opsporen en bestrijden van valse claims van deelname aan het kader, bijvoorbeeld door het uitvoeren van zoekopdrachten op internet[14].

Bij het houden van toezicht op de naleving van de DPF-beginselen door DPF-gecertificeerde bedrijven heeft het ministerie van Handel het afgelopen jaar voornamelijk vertrouwd op het uitvoeren van ad-hoczoekopdrachten op internet en het monitoren van (sociale) media. Het ministerie heeft gerapporteerd dat het in dit eerste jaar geen problemen met de naleving van de DPF-beginselen heeft vastgesteld en ook geen bedrijven heeft doorverwezen naar de FTC of het ministerie van Vervoer voor mogelijke handhavingsmaatregelen. Ook heeft het ministerie een speciaal contactpunt opgezet om de samenwerking met gegevensbeschermingsautoriteiten te vergemakkelijken en klachten van personen en verwijzingen van andere autoriteiten (bv. gegevensbeschermingsautoriteiten of de FTC) te ontvangen. Het afgelopen jaar zijn echter geen verwijzingen of klachten binnengekomen. Waar in dit eerste jaar van werking van het DPF de focus ligt op het opzetten van het kader en het certificeringsproces, heeft het ministerie van Handel tijdens de evaluatievergadering uitgelegd dat het voornemens is de nalevingscontroles te automatiseren om deze op een meer systematische manier te kunnen uitvoeren en dat het momenteel de daartoe benodigde IT-instrumenten ontwikkelt.

De Commissie erkent dat het ministerie van Handel zijn inspanningen in dit eerste jaar moest richten op het opzetten van het kader en het certificeringsproces. Voor de toekomst is het belangrijk dat het ministerie van Handel meer doet om de naleving van de beginselen te monitoren en te controleren, wat nodig is om een hoog niveau van naleving van het kader te waarborgen en gevallen die handhavingsmaatregelen vereisen op te sporen, met inbegrip van mogelijke valse claims van deelname door bedrijven. In dit verband is de Commissie verheugd dat het ministerie van Handel heeft bevestigd dat het van plan is (geautomatiseerde) instrumenten te ontwikkelen en te gebruiken om nalevingsproblemen en valse claims doeltreffender en op meer systematische wijze op te sporen. De Commissie is van mening dat dit deel zou moeten uitmaken van een bredere inspanning om op grotere schaal gebruik te maken van de verschillende beschikbare instrumenten (zoals steekproefsgewijze controles, nalevingsvragenlijsten, informatieverzoeken enz.), onder meer om de naleving van specifieke vereisten van het DPF te verifiëren[15].

DPF-organisaties vallen onder de jurisdictie van de FTC en het ministerie van Handel van de VS. Tijdens de evaluatievergadering heeft het ministerie bevestigd dat het beschikt over alle procedures om passende handhavingsmaatregelen te nemen. Ook heeft het ministerie

[14] Zie bijlage III bij het adequaatheidsbesluit. Van valse claims kan bijvoorbeeld sprake zijn wanneer een bedrijf beweert deel te nemen aan het DPF, maar nooit het certificeringsproces is gestart, dat proces niet heeft voltooid of zijn certificering heeft laten verlopen.

[15] Bijvoorbeeld met betrekking tot verdere doorgiften, door gebruik te maken van de mogelijkheid om op grond van DPF-beginsel 3.b. te verzoeken om een samenvatting of een representatief exemplaar van de gegevensbeschermingsbepalingen van de overeenkomst inzake verdere doorgiften.

toegelicht dat zeer weinig bedrijven die onder zijn jurisdictie vallen zich bij het DPF hebben aangesloten (enkele reisbureaus, maar geen luchtvaartmaatschappijen). De FTC heeft bevestigd dat zij in elk van haar gegevensbeschermingsonderzoeken systematisch controles op schendingen van het DPF uitvoert. Tot dusver heeft de FTC geen verwijzingen van andere autoriteiten ontvangen. Wel zijn er enkele klachten ontvangen waarin het DPF werd genoemd, waarvan er echter twee betrekking hadden op bedrijven die op de "inactieve lijst" stonden en twee op bedrijven die niet deelnamen aan het kader, terwijl één klacht geen betrekking had op persoonsgegevens die vanuit de EU waren doorgegeven. Ten tijde van het opstellen van dit verslag had de FTC nog geen handhavingsbesluiten uit hoofde van het DPF uitgevaardigd, al heeft zij bevestigd dat er momenteel onderzoeken naar verschillende DPF-gecertificeerde bedrijven lopen.

De Commissie is ingenomen met het feit dat de FTC in al haar privacyonderzoeken systematisch controleert op schendingen van het DPF. Aangezien de blijvende doeltreffendheid van het DPF afhangt van een robuuste handhaving ervan, wordt verwacht dat de FTC nadere invulling zal geven aan haar onderzoeksbevoegdheden uit hoofde van het kader, onder meer door proactief bezemacties uit te voeren met een focus op de naleving van specifieke DPF-vereisten en/of op bepaalde sectoren.

2.1.3. Behandeling van klachten

Het DPF biedt EU-burgers verschillende verhaalsmogelijkheden in geval van niet-naleving van de DPF-beginselen door gecertificeerde organisaties[16]. Een daarvan is het nastreven van een oplossing door middel van rechtstreekse contacten met de DPF-gecertificeerde organisatie, die de getroffen persoon binnen 45 dagen moet antwoorden. Betrokkenen kunnen ook een klacht indienen via het verhaalsmechanisme dat door een organisatie is aangewezen voor het onderzoeken en beslechten van klachten. Afhankelijk van de omstandigheden kan dit een particuliere geschillenbeslechtingsinstantie of een gegevensbeschermingsautoriteit zijn[17]. Ten slotte kunnen betrokkenen, indien geen van de andere beschikbare mogelijkheden van het verhaalsmechanisme heeft geleid tot een bevredigende beslechting van hun klacht, in laatste instantie verzoeken om bindende arbitrage voor het EU-VS-DPF-panel.

2.1.3.1. Behandeling van klachten door bedrijven

Uit de antwoorden van brancheorganisaties en bedrijven op de door de Commissie toegezonden vragenlijsten blijkt dat DPF-gecertificeerde bedrijven zeer weinig tot geen klachten van particulieren over niet-naleving van de DPF-beginselen hebben ontvangen. Tegelijkertijd hebben bedrijven verschillende mechanismen en instrumenten opgetuigd om personen in staat te stellen hun rechten uit te oefenen en klachten in te dienen, bijvoorbeeld door middel van webformulieren, per e-mail of telefonisch.

2.1.3.2. *Onafhankelijke verhaalsmechanismen*

Uit de feedback die tijdens de evaluatievergadering is ontvangen en uit de informatie die door brancheorganisaties is verstrekt, blijkt dat er een zeer laag aantal klachten is ingediend bij onafhankelijke verhaalsmechanismen. Door bedrijven gekozen verhaalsmechanismen zijn

[16] Zie punt 2.4 van het adequaatheidsbesluit.

[17] DPF-organisaties zijn verplicht om mee te werken aan het onderzoek en het oplossen van een klacht door een gegevensbeschermingsautoriteit wanneer de klacht betrekking heeft op de verwerking van personeelsgegevens die in het kader van een arbeidsverhouding zijn verzameld of wanneer de betrokken organisatie zich vrijwillig aan het toezicht van gegevensbeschermingsautoriteiten heeft onderworpen.

onder meer BBB National Programs, JAMS, TRUSTe en VeraSafe. Het DPF vereist dat de verhaalsmechanismen een jaarverslag met geaggregeerde statistieken over het gebruik van hun geschillenbeslechtingsdiensten publiceren. Ten tijde van de vaststelling van dit verslag hadden alle betrokken verhaalsmechanismen hun jaarverslag gepubliceerd[18].

Bovendien hebben BBB en VeraSafe tijdens de evaluatievergadering uitvoerige presentaties over hun activiteiten in het afgelopen jaar gegeven. Daarbij maakten zij melding van een groter aantal deelnemende bedrijven dat voor hun diensten had gekozen in vergelijking met eerdere kaders en merkten zij op dat zij wel klachten hadden ontvangen, maar dat de overgrote meerderheid daarvan niet-ontvankelijk was verklaard. Zo had BBB 87 klachten van EU-burgers ontvangen, waarvan er echter slechts twee in aanmerking kwamen voor beslechting. BBB legde uit dat klachten gemiddeld binnen vijf werkdagen worden verwerkt, maar dat die twee klachten uiteindelijk waren afgesloten vanwege het uitblijven van een reactie van de betrokkenen. VeraSafe had 26 klachten ontvangen, waarvan er zes in aanmerking kwamen voor beslechting. Twee van de klachten die betrekking hadden op verzoeken om toegang en verwijdering zijn beslecht, twee zijn nog in behandeling en twee zijn ingetrokken of afgesloten als gevolg van het uitblijven van aan reactie van de betrokkene. Beide organisaties lichtten toe dat zij ernaar streven om klachten te beantwoorden in de taal van de klager.

DPF-gecertificeerde bedrijven die vanuit de EU doorgegeven personeelsgegevens verwerken, moeten de gegevensbeschermingsautoriteiten van de EU selecteren als hun onafhankelijke verhaalsmechanisme voor die gegevens, terwijl zij voor andere soorten persoonsgegevens die in het kader van het DPF worden doorgegeven op vrijwillige basis de EU-gegevensbeschermingsautoriteiten kunnen selecteren als hun onafhankelijke verhaalsmechanisme. Meer dan de helft van de bedrijven die ten tijde van de evaluatie DPF-gecertificeerd waren, had voor deze oplossing gekozen[19], hetgeen wordt verwelkomd. Na de vaststelling van het adequaatheidsbesluit heeft de EDPB het reglement van orde voor het "informeel panel van gegevensbeschermingsautoriteiten op EU-niveau" vastgesteld. Het panel is bevoegd voor het verstrekken van bindend advies aan Amerikaanse organisaties over onbeslechte klachten van betrokkenen over de behandeling van persoonsgegevens die in het kader van het DPF zijn doorgegeven vanuit de EU. Volgens het reglement van orde bestaat het panel uit een gegevensbeschermingsautoriteit die optreedt als leidende gegevensbeschermingsautoriteit en andere aangewezen gegevensbeschermingsautoriteiten, die

[18] ANA — https://www.ana.net/content/show/id/accountability-dpf-consumers;
BBB National Programs — https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf; ICDR — AAA — https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0;
Insights association — https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS — https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf;
Privacy Trust DPF Services — https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf;
TRUSTe Dispute Resolution — https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf;
Verasafe — https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

[19] Kort na de datum van de evaluatievergadering werd op de DPF-website vermeld dat 1 511 van de 2 892 deelnemers een EU-gegevensbeschermingsautoriteit hadden gekozen als verhaalsmechanisme.

gezamenlijk het advies opstellen[20]. Het bindend advies moet binnen zestig dagen na ontvangst van een DPF-klacht worden verstrekt. De EDPB heeft ook een modelklachtenformulier gepubliceerd voor het indienen van klachten bij gegevensbeschermingsautoriteiten[21], evenals documenten met veelgestelde vragen en antwoorden over het DPF voor Europese natuurlijke personen ("EU-U.S. DPF FAQ for European individuals")[22] en bedrijven ("EU-U.S. DPF FAQ for European businesses")[23]. Ten tijde van de evaluatie had het panel nog geen klachten ontvangen.

2.1.3.3. Het mechanisme van bindende arbitrage

Het International Centre for Dispute Resolution (ICDR), de internationale afdeling van de American Arbitration Association, is door het ministerie van Handel van de VS geselecteerd om het mechanisme van bindende arbitrage te beheren. Na de vaststelling van het adequaatheidsbesluit heeft het ministerie samen met de Commissie elf arbiters met ervaring op het gebied van gegevensbescherming en met verschillende achtergronden, waaronder arbitrage, de rechterlijke macht, de academische wereld en het maatschappelijk middenveld, geselecteerd[24]. Daarnaast zijn de arbitrageregels[25] voor het DPF-panel en een gedragscode voor arbiters[26] vastgesteld, die beschikbaar zijn op de website van het ICDR. Ten tijde van de evaluatie had nog geen enkele natuurlijke persoon in de EU een beroep op het arbitragemechanisme gedaan.

2.1.4. Richtsnoeren, samenwerking en bewustmaking

Sinds de inwerkingtreding van het DPF heeft het ministerie van Handel van de VS diverse bewustmakingsactiviteiten uitgevoerd, waaronder roadshows, webinars en conferenties. Daarnaast zijn er contacten gelegd met brancheorganisaties en is aan meer dan drieduizend bedrijven rechtstreeks informatie over het DPF verstrekt. Het ministerie heeft ook richtsnoeren gepubliceerd, onder meer in de vorm van veelgestelde vragen en de bijbehorende antwoorden voor natuurlijke personen en bedrijven in de EU en de VS[27]. De EDPB heeft op zijn beurt klachtenformulieren en documenten met veelgestelde vragen en de bijbehorende antwoorden ontwikkeld voor natuurlijke personen en bedrijven. Evenzo heeft de Commissie bij de vaststelling van haar adequaatheidsbesluit een document met veelgestelde vragen en de bijbehorende antwoorden alsmede een factsheet over het DPF gepubliceerd[28].

[20] Het reglement van orde voor het "informeel panel van gegevensbeschermingsautoriteiten op EU-niveau" is door de EDPB op 17 april 2024 vastgesteld overeenkomstig het EU-VS-kader voor gegevensbescherming. Het reglement van orde is hier te vinden: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.

[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_en.

[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_en.

[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_en.

[24] https://go.adr.org/DPF_Arbitrator_Bios.html.

[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.

[26] https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.

[27] Zie bv. https://www.dataprivacyframework.gov/US-Businesses.

[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

Tegelijkertijd is uit de evaluatievergadering naar voren gekomen dat er meer moet worden gedaan om het bewustzijn onder natuurlijke personen te vergroten en bedrijven te voorzien van richtsnoeren. De van bedrijven en onafhankelijke verhaalsmechanismen ontvangen input en het zeer lage aantal klachten duiden erop dat natuurlijke personen niet altijd op de hoogte zijn van hun rechten en/of van het mechanisme om die rechten uit te oefenen. Tijdens de evaluatievergadering heeft het ministerie van Handel belangstelling getoond voor samenwerking met de gegevensbeschermingsautoriteiten van de EU om de kennis over het kader onder EU-burgers te vergroten. De Commissie moedigt dergelijke initiatieven aan en onderneemt zelf ook stappen om natuurlijke personen beter te informeren, onder meer door aanvullende informatie over het DPF te verstrekken op haar website, bijvoorbeeld door middel van links en verwijzingen naar relevante richtsnoeren van de EDPB en het ministerie van Handel en andere autoriteiten van de VS.

Wat betreft het verstrekken van richtsnoeren inzake de DPF-beginselen, hebben de vertegenwoordigers van de EDPB tijdens de evaluatievergadering toegezegd de komende maanden mee te werken aan een verdere verduidelijking van het begrip "personeelsgegevens" zoals gebruikt in het DPF en van de specifieke verplichtingen die van toepassing zijn op de verwerking van zulke gegevens. Daartoe werden verschillende in die richtsnoeren op te nemen elementen onder de loep genomen. Zo zou in de richtsnoeren kunnen worden ingegaan op bepaalde praktische DPF-scenario's waarin werknemersgegevens worden verwerkt (bijvoorbeeld door een cloudprovider) en kunnen worden toegelicht welke DPF-verplichtingen voor die scenario's relevant zijn. Ook zou aan bedrijven die werknemersgegevens van EU-burgers ontvangen (zonder die noodzakelijkerwijs te gebruiken in het kader van een arbeidsverhouding) de suggestie kunnen worden gedaan om het panel van gegevensbeschermingsautoriteiten te kiezen als hun verhaalsmechanisme. Dit zou ervoor zorgen dat die burgers zich kunnen wenden tot een autoriteit die "dichtbij" hen staat en indien nodig beter bekend is met de nationale wetgeving die van toepassing is op personeelsgegevens.

Een specifiek gebied waarop bijkomende richtsnoeren nuttig lijken te zijn (ook gezien de input van brancheorganisaties) is dat van de DPF-vereisten voor verdere doorgiften. Ook heeft het ministerie van Handel opgemerkt dat het de moeite waard zou zijn om na te gaan of bepaalde sectoren baat zouden kunnen hebben bij aanvullende richtsnoeren inzake de toepassing van de DPF-beginselen op hun activiteiten, bijvoorbeeld op het gebied van gezondheidsonderzoek en financiële diensten.

De Commissie verwelkomt de bereidheid van beide partijen om richtsnoeren te ontwikkelen en verwacht dat de werkzaamheden ten aanzien van bovengenoemde onderwerpen spoedig van start zullen gaan.

Meer in het algemeen zijn er verschillende mechanismen voor uitwisselingen en samenwerking tussen de Amerikaanse autoriteiten en EU-gegevensbeschermingsautoriteiten opgezet, onder meer door de aanwijzing van speciale contactpersonen binnen de FTC en het ministerie van Handel om vragen en verwijzingen van gegevensbeschermingsautoriteiten te behandelen.

2.1.5. Relevante ontwikkelingen in het rechtsstelsel van de VS

Sinds de vaststelling van het adequaatheidsbesluit hebben zich een aantal ontwikkelingen in het rechtskader van de VS op het gebied van gegevensbescherming voorgedaan, waaronder ontwikkelingen op het gebied van wet- en regelgeving en jurisprudentie. Deze ontwikkelingen duiden over het algemeen op een grotere convergentie tussen de benaderingen van de EU en

de VS van bepaalde uitdagingen met betrekking tot gegevensbescherming, onder meer door het gebruik van vergelijkbare juridische begrippen. Sommige van deze ontwikkelingen zijn nog lopende en zullen verder moeten worden gemonitord.

Op federaal niveau heeft de president van de VS verschillende Executive Orders (presidentiële besluiten) uitgevaardigd die relevant zijn voor het gebruik van persoonsgegevens. Executive Order 14117 van 28 februari 2024[29] verbiedt of beperkt transacties met bepaalde categorieën gevoelige persoonsgegevens (zoals gezondheidsgegevens, biometrische identificatiemiddelen, gegevens over het menselijk genoom) met entiteiten in bepaalde "zorgwekkende landen"[30]. In het presidentiële besluit wordt de minister van Justitie opgedragen om ontwerpregelgeving in te dienen — wat op het moment van de vaststelling van dit verslag nog niet was gebeurd — waarin de uitvoering ervan nader wordt gespecificeerd. Executive Order 14110 van 30 oktober 2023 inzake kunstmatige intelligentie[31] ziet op de ontwikkeling van veilige, beveiligde en betrouwbare kunstmatige intelligentie. In dit presidentiële besluit wordt van verschillende federale agentschappen verlangd dat zij AI-gerelateerde veiligheidsnormen en -richtsnoeren ontwikkelen, onder meer inzake specifieke AI-risico's voor de privacy en privacybeschermende technieken.

Op wetgevingsgebied zijn de afgelopen jaren federale privacywetten ingediend bij het Congres, maar hebben twintig Amerikaanse staten met ingang van juli 2024 zelf uitgebreide privacywetten aangenomen, waarvan er acht in werking zijn getreden: in Californië, Colorado, Oregon, Virginia, Connecticut, Utah, Texas en Florida. Daarnaast hebben 17 Amerikaanse staten wetgeving inzake geautomatiseerde verwerking (of althans enkele vormen ervan) ingevoerd, die in de meeste gevallen ruimte laat voor opt-outs voor bepaalde soorten besluitvorming op basis van "profilering"[32].

Wat de ontwikkelingen in de jurisprudentie betreft, hebben verschillende vertegenwoordigers van het maatschappelijk middenveld gewezen op het recente arrest van de Supreme Court (hoogste rechterlijke instantie van de VS) in de zaak Loper Bright Enterprises v. Raimondo (van 28 juni 2024). Dit arrest heeft een streep gezet door eerdere rechtspraak op basis van de

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] Deze zorgwekkende landen zijn, zoals voorgesteld door de minister van Justitie van de VS in een vooraankondiging van 3 mei 2024 van voorgestelde regelgeving, China, Cuba, Hong Kong en Macau, Iran, Noord-Korea en Venezuela. Zie https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[32] Hoewel de verschillende staten uiteenlopende betekenissen van het begrip "profilering" hanteren, wordt profilering over het algemeen gedefinieerd als elke vorm van geautomatiseerde verwerking van persoonsgegevens om persoonlijke aspecten die verband houden met de economische situatie, de gezondheid, de persoonlijke voorkeuren, de interesses, de betrouwbaarheid, het gedrag, de locatie of de bewegingen van een geïdentificeerde of identificeerbare natuurlijke persoon te evalueren, te analyseren of te voorspellen. Doorgaans zijn het consumenten die voor een opt-out voor profilering kunnen kiezen. De volgende Amerikaanse staten hebben wetgeving inzake profilering ontwikkeld: Colorado (Colo. Rev. Stat. Ann. § 6-1-1306), Connecticut (Conn. Gen. Stat. Ann. § 42-518), Delaware (Del. Code Ann. tit. 6, § 12D-104), Florida (Fla. Stat. Ann. § 501.705), Indiana (Ind. Code Ann. § 24-15-3-1), Kentucky (Ky. Rev. Stat. Ann. § 367.3615), Maryland (Maryland Online Data Privacy Act of 2024, vastgesteld op 9 mei 2024), Minnesota (Minn. Stat. Ann. § 325O.07), Montana (Mont. Code Ann. § 30-14-2808), Nebraska (Neb. Rev. Stat. Ann. § 87-1107), New Hampshire (N.H. Rev. Stat. Ann. § 507-H:4), New Jersey (N.J. Stat. Ann. § 56:8-166.8), Oregon (Or. Rev. Stat. Ann. § 646A.574), Rhode Island (Rhode Island Data Transparency and Privacy Protection Act, vastgesteld op 29 juni 2024), Tennessee (Tenn. Code Ann. § 47-18-3304), Texas (Tex. Bus. & Com. Code Ann. § 541.051), en Virginia (Va. Code Ann. § 59.1-577).

Chevron-doctrine, die inhoudt dat rechters het beginsel van eerbied ("deference") moeten toepassen op de redelijke interpretatie van de wet door een toezichthoudende instantie in geval van dubbelzinnige wetgeving die door die instantie wordt gehandhaafd. Enkele ngo's hebben hun zorgen geuit over de gevolgen van deze uitspraak van de Supreme Court voor de regelgevende bevoegdheid van de FTC op het gebied van gegevensbescherming, waarbij zij erkennen dat de handhavingsbevoegdheden van de FTC mogelijk niet of hoogstens in beperkte mate in het geding zijn. Tijdens de evaluatievergadering heeft de FTC verklaard dat het nog te vroeg is om de precieze implicaties van dit arrest te kunnen vaststellen. Tegelijkertijd heeft de FTC uitgelegd dat haar regelgevingsactiviteiten onder een andere bevoegdheid in de FTC Act vallen dan die van andere bestuursorganen en dat de Chevron-doctrine voor die activiteiten minder relevant was. Bijgevolg zal het recente arrest mogelijk beperkte gevolgen op dit gebied hebben.

Daarnaast heeft de FTC de deelnemers aan de vergadering bijgepraat over recente ontwikkelingen in haar benadering van geautomatiseerde verwerking en kunstmatige intelligentie. Deze omvatten de publicatie, met andere handhavingsautoriteiten, van een gezamenlijke verklaring tegen discriminatie en vooringenomenheid in geautomatiseerde systemen[33] en de vaststelling van verschillende handhavingsmaatregelen — waarbij de FTC onder meer focust op transparantie, de eerlijkheid van geautomatiseerde verwerking en het vermogen van natuurlijke personen om de uitkomsten van verwerkingen aan te vechten. Het meest opvallende besluit van de FTC in dit verband betreft dat van maart 2024 waarbij Rite Aid een verbod van vijf jaar op het gebruik van gezichtsherkenningstechnologie voor beveiligingsdoeleinden werd opgelegd[34]. De FTC oordeelde dat Rite Aid geen redelijke maatregelen had genomen om foutieve resultaten te voorkomen en consumenten te informeren over de toegepaste technologie. Meer in het algemeen heeft de FTC tijdens de evaluatievergadering een overzicht van haar huidige prioriteiten gegeven, en met name van de gebieden die in haar opvatting in de toekomst een meer proactieve handhavingsaanpak verdienen. Daartoe behoren de bescherming van gevoelige gegevens (gezondheids-, biometrische, geolocatiegegevens enz.) [35], de bescherming van kinderen[36] en minderjarigen online, en gegevensbeveiliging[37].

De Commissie zal deze en andere ontwikkelingen in de VS nauwlettend blijven volgen, met name eventuele verdere stappen in de richting van een alomvattende federale privacywet en de mogelijke gevolgen van de recente rechtspraak van de Supreme Court voor de rol van de FTC op het gebied van gegevensbescherming.

---

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

[35] Zie bijvoorbeeld de recente besluiten van de FTC tegen X-Mode voor het verkopen en delen van gevoelige locatie-informatie (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) en tegen Monument met betrekking tot de doorgifte van gevoelige gezondheidsgegevens aan derden voor marketingdoeleinden (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] Zo heeft de FTC recentelijk een onderzoek aangekondigd dat moet leiden tot een gerechtelijke procedure tegen TikTok en zijn moederbedrijf Bytedance wegens inbreuk op de wetgeving inzake de privacy van kinderen. Volgens de FTC hebben beide bedrijven niet voldaan aan het vereiste om de ouders te informeren en hun toestemming te verkrijgen voordat zij persoonlijke informatie van kinderen van jonger dan 13 jaar verzamelen en gebruiken (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Zie het overzicht van recente handhavingsactiviteiten in "FTC 2023 Privacy and Data Security Update 2023": https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307.

De Commissie verwelkomt de informatie die de FTC heeft verstrekt over haar recente handhavingsactiviteiten en huidige prioriteiten, die grotendeels aansluiten bij trends en prioriteiten op het gebied van handhaving van gegevensbescherming in de EU. De FTC neemt ook actief deel aan het netwerk van landen die profiteren van de voordelen van een EU-adequaatheidsbesluit, dat de Commissie in maart 2024 heeft opgezet[38]. Deze grotere convergentie zou een nauwere samenwerking tussen gegevensbeschermingshandhavingsinstanties aan beide zijden van de Atlantische Oceaan moeten bevorderen en vergemakkelijken, met name in aangelegenheden die relevant zijn voor de werking van het DPF.

2.2. Aspecten van de toegang tot en het gebruik door Amerikaanse overheidsinstanties van uit hoofde van het DPF doorgegeven persoonsgegevens

Het adequaatheidsbesluit bevat een gedetailleerde beoordeling van de regels die van toepassing zijn op het verzamelen en het gebruik door Amerikaanse overheidsinstanties van uit de EU aan DPF-gecertificeerde bedrijven doorgegeven persoonsgegevens, met name voor de rechtshandhaving en ten behoeve van de nationale veiligheid. Zoals de Amerikaanse autoriteiten tijdens de evaluatievergadering hebben bevestigd, hebben zich sinds de vaststelling van het adequaatheidsbesluit, in het eerste jaar van het DPF, geen relevante ontwikkelingen voorgedaan in het rechtskader dat van toepassing is op de toegang tot gegevens voor rechtshandhavings- of regelgevingsdoeleinden. Om die reden hebben onderstaande bevindingen alleen betrekking op ontwikkelingen op het gebied van nationale veiligheid.

De conclusies in het adequaatheidsbesluit inzake de toegang van inlichtingendiensten tot gegevens stoelen op een analyse van de voorwaarden en beperkingen die van toepassing zijn op inlichtingen uit berichtenverkeer (signals intelligence, “SIGINT”) door verschillende justitiële autoriteiten — met name de voorwaarden en beperkingen van artikel 702 van de Foreign Intelligence Surveillance Act (FISA) en Executive Order 12333[39] — zoals aangevuld en versterkt door Executive Order 14086 “Enhancing Safeguards for US Signals Intelligence Activities” (Versterken van de waarborgen voor SIGINT-activiteiten van de VS) van de president van de VS van 7 oktober 2022. De waarborgen van EO 14086 zijn van toepassing op alle SIGINT-activiteiten van de VS, ongeacht de justitiële autoriteit onder wier bevoegdheid de activiteit plaatsvindt en ongeacht waar de activiteit plaatsvindt, en beschermen de gegevens van niet-Amerikaanse personen (waaronder Europeanen)[40]. EO 14086 heeft ook een nieuw verhaalsmechanisme ingesteld waarmee deze bindende waarborgen kunnen worden ingeroepen en afgedwongen door natuurlijke personen in de EU.

[38] Zie https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307. De vergadering van maart 2024 heeft geleid tot een besluit om een reeks thematische sessies te houden. De eerste sessie heeft plaatsgevonden in juli 2024 en was gericht op het ontwikkelen van instrumenten die kleine en middelgrote ondernemingen kunnen ondersteunen bij het naleven van privacywetten.

[39] Andere maatregelen die op grond van de FISA kunnen worden genomen met betrekking tot gegevens die vanuit de EU worden doorgegeven, zijn geïndividualiseerd elektronisch toezicht (artikel 105 FISA), het uitvoeren van fysieke zoekopdrachten (artikel 302 FISA), het gebruik van trackers van berichtenverkeer (artikel 402 FISA) en het verzamelen van bedrijfsgegevens van bepaalde bedrijven (algemene vervoerbedrijven, openbare accommodaties, autoverhuurfaciliteiten of opslagfaciliteiten, artikel 501 FISA). Deze verschillende rechtsgrondslagen worden uitvoerig geanalyseerd in het adequaatheidsbesluit (overwegingen 142 tot en met 152).

[40] Voor meer informatie, zie punt 3.2.1.2 van het adequaatheidsbesluit.

In de paragrafen hieronder wordt een overzicht gegeven van de stappen die de Amerikaanse autoriteiten sinds de vaststelling van het adequaatheidsbesluit hebben genomen om EO 14086 na te leven en van relevante ontwikkelingen met betrekking tot bovengenoemd rechtskader.

2.2.1. Relevante ontwikkelingen met betrekking tot het rechtskader van de VS

2.2.1.1. Uitvoering van Executive Order 14086 door inlichtingendiensten

De bij EO 14086 ingevoerde beperkingen en waarborgen vormen een aanvulling op de beperkingen en waarborgen van artikel 702 FISA en EO 12333. Zij zijn bindend voor alle inlichtingendiensten en zijn door elke afzonderlijke dienst verder geoperationaliseerd door middel van beleidsdocumenten en procedures.

In het kader van deze eerste evaluatie hebben de Amerikaanse autoriteiten bevestigd dat EO 14086 sinds de vaststelling ervan niet is gewijzigd. Voorts is verduidelijkt dat de president van de VS geen gebruik heeft gemaakt van de in de artikelen 2, (b), (i), (B) en 2, (b), (ii), (C), van EO 14086 voorziene bevoegdheid om de lijst van legitieme doelstellingen die kunnen worden nagestreefd met SIGINT-activiteiten, of de lijst van doeleinden waarvoor bulksgewijs verzamelde gegevens kunnen worden gebruikt, bij te werken[41]. Voor het nader bepalen van de prioriteiten waarvoor inlichtingen uit berichtenverkeer kunnen worden verzameld, is bij EO 14086 een specifieke procedure ingevoerd. Meer bepaald moet de functionaris voor de bescherming van de burgerlijke vrijheden (Civil Liberties Protection Officer) van het bureau van de directeur voor de nationale inlichtingendiensten (Office of the Director of National Intelligence) (hierna "CLPO van het ODNI" genoemd) worden geraadpleegd om voor elke prioriteit te beoordelen of deze 1) een of meer in de EO genoemde legitieme doelstellingen bevordert; 2) niet is bedoeld voor of naar verwachting zal resulteren in het verzamelen van SIGINT voor een in de EO genoemd verboden doel; en 3) is vastgesteld met inachtneming van de privacy en de burgerlijke vrijheden van alle personen[42]. Tijdens de evaluatievergadering heeft de CLPO van het ODNI bevestigd dat hij een beoordeling heeft uitgevoerd van de door de directeur voor de nationale inlichtingendiensten in het kader voor de nationale inlichtingenprioriteiten (National Intelligence Priorities Framework) 2023 van de VS voorgestelde prioriteiten, heeft geconcludeerd dat deze aan de hierboven genoemde vereisten voldeden en zijn conclusie heeft gedeeld met de directeur voor de nationale inlichtingendiensten, die de prioriteiten op zijn beurt heeft voorgelegd aan de president van de VS voor validatie. De CLPO van het ODNI heeft ook opleidingen over de vereisten van EO 14086 georganiseerd voor medewerkers van onderdelen van de inlichtingendiensten die betrokken zijn bij de ontwikkeling van inlichtingenprioriteiten.

Daarnaast hebben de Amerikaanse autoriteiten het afgelopen jaar verdere praktische stappen ondernomen om EO 14086 te integreren in hun dagelijkse activiteiten. Met name hebben de inlichtingendiensten verdere interne beleidslijnen en richtsnoeren voor de toepassing van de EO ingevoerd, zoals interne processen (op basis van interne autorisatievereisten, gedocumenteerde toegangscontroles, zodat alleen personen die naar behoren zijn opgeleid en over de benodigde missievereisten beschikken, toegang tot de informatie hebben enz.) om te waarborgen dat de vereisten inzake noodzakelijkheid en evenredigheid in acht worden

[41] Deze legitieme doelstellingen/doeleinden zijn bijvoorbeeld bescherming tegen spionage, sabotage en moordaanslagen, tegen andere inlichtingenactiviteiten die worden uitgevoerd door, namens of met hulp van een buitenlandse regering, organisatie of persoon, en tegen terrorisme, het nemen van gijzelaars en het gevangen houden van personen door of namens een buitenlandse regering, organisatie of persoon.
[42] Artikel 2, (b), (iii), EO 14086.

genomen in het kader van zowel gerichte als bulksgewijze verzameling[43]. Bovendien zijn er opleidingen over EO 14086 verstrekt aan personeel van verschillende inlichtingendiensten (zoals de NSA, de CIA, de FBI), waaronder door de CLPO van het ODNI georganiseerde jaarlijkse en ad-hocopleidingssessies en verplichte opleidingen voor alle nieuwe medewerkers van het ODNI.

De Commissie is ingenomen met de verschillende maatregelen die zijn genomen om uitvoering aan EO 14086 te geven en de naleving ervan te waarborgen. Wanneer er meer ervaring is opgedaan met de praktische toepassing van de waarborgen van de EO, zou de Commissie het op prijs stellen om in het kader van toekomstige evaluaties concrete voorbeelden van de werking van de EO in de praktijk (met inachtneming van de toepasselijke vertrouwelijkheidsvereisten) te bespreken.

2.2.1.2. Hernieuwde goedkeuring van artikel 702 FISA

Artikel 702 FISA maakt het mogelijk om buitenlandse inlichtingen te verwerven over personen van wie redelijkerwijs kan worden aangenomen dat zij zich buiten de VS bevinden. De verwerving vindt plaats op basis van jaarlijkse certificeringen die moeten worden ingediend bij en goedgekeurd door de Foreign Intelligence Surveillance Court (rechtbank voor buitenlandse-inlichtingensurveillance van de VS) (FISC). Deze certificeringen hebben betrekking op specifieke categorieën van te verzamelen buitenlandse inlichtingen. Op 21 juli 2023 heeft het ODNI bekendgemaakt dat er drie certificeringen waren goedgekeurd uit hoofde van artikel 702 FISA, die de volgende categorieën buitenlandse inlichtingen bestrijken: 1) buitenlandse regeringen en aanverwante entiteiten, 2) terrorismebestrijding, en 3) bestrijding van proliferatie[44]. De certificeringen moeten ook voorzien in door de FISC goedgekeurde procedures om het doelwit te specificeren ("targeting") en minimaliseringsprocedures[45]. Specifiek wordt het vaststellen van doelwitten uitgevoerd via verzoeken aan Amerikaanse bedrijven die onder de FISA-definitie van "aanbieder van elektronische-communicatiediensten" vallen om overlegging van elektronische-communicatiegegevens van communicatie die wordt verzonden naar of van zogenoemde "selectietermen" (die een specifieke communicatieaccount identificeren, zoals een telefoonnummer of een e-mailadres). De Amerikaanse regering heeft een aantal documenten over artikel 702 FISA gepubliceerd om het publiek te informeren over de werking van surveillanceprogramma's, de toepasselijke vereisten, de waarborgen voor de privacy en de rol van de FISC[46].

Als gevolg van een vervalclausule zou artikel 702 FISA eind 2023 komen te vervallen, tenzij het opnieuw zou worden goedgekeurd door het Congres. Na een tijdelijke hernieuwde goedkeuring zonder wijzigingen, heeft het Congres op 19 april 2024 de Reforming Intelligence and Securing America Act (wet tot herziening van de inlichtingenwetgeving en tot bescherming van de veiligheid van de VS) (RISAA) aangenomen, waarbij artikel 702 FISA opnieuw is bekrachtigd voor een periode van twee jaar, met een aantal wijzigingen. Die wijzigingen

[43] Zie https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, gepubliceerd op 3 juli 2023.
[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.
[45] Die procedures beperken het verzamelen van gegevens met betrekking tot een specifiek doel van buitenlandse inlichtingen, begrenzen de toegang tot databanken waarin overeenkomstig artikel 702 FISA verkregen informatie is opgeslagen (onder meer door middel van toegangscontroles) en leggen restricties op aan het gebruik, de bewaring en de verspreiding van die informatie.
[46] https://www.intel.gov/foreign-intelligence-surveillance-act.

kunnen grofweg worden onderverdeeld in twee categorieën: 1) wijzigingen in het toepassingsgebied van door artikel 702 FISA toegestane surveillanceactiviteiten; en 2) institutionele en procedurele wijzigingen.

Wijzigingen van het toepassingsgebied van surveillanceactiviteiten die zijn toegestaan op grond van artikel 702 FISA

De RISAA heeft gezorgd voor drie belangrijke wijzigingen van het toepassingsgebied van surveillanceactiviteiten die op grond van artikel 702 FISA kunnen worden uitgevoerd.

In de eerste plaats is het verzamelen van zogeheten "abouts" (indirecte gegevens) definitief verboden[47]. Dit begrip heeft betrekking op het verzamelen van communicatie waarbij in het "aan" of "van" van de communicatie niet een selectieterm van artikel 702 FISA (zoals een e-mailadres) wordt vermeld, maar in de eigenlijke communicatie naar een dergelijke selectieterm wordt verwezen (waarbij kan worden gedacht aan bijvoorbeeld e-mailcommunicatie die niet naar of van het geselecteerde e-mailadres is verzonden, maar waarin het geselecteerde e-mailadres is opgenomen in de hoofdtekst van de e-mail). Ofschoon deze vorm van gegevensverzameling reeds was uitgesloten na een wijziging van de FISA in 2018, voorzag de FISA nog steeds in de mogelijkheid om de verzameling van "abouts" in de toekomst te hervatten na een specifieke goedkeuringsprocedure met betrokkenheid van de FISC en het Congres. Deze mogelijkheid is door de RISAA geschrapt.

In de tweede plaats is de definitie van "buitenlandse inlichtingen" uitgebreid met informatie inzake de bestrijding van illegale drugshandel[48]. Tijdens de evaluatievergadering hebben de Amerikaanse autoriteiten toegelicht dat deze uitbreiding is ingevoerd in het licht van de huidige fentanylcrisis en de toenemende dreiging die internationale drugshandelaren en -fabrikanten vormen voor de nationale veiligheid. Tegen deze achtergrond werd bevestigd dat dit begrip onder verschillende van de EO 14086 vermelde legitieme doelstellingen valt, te weten het begrijpen of beoordelen van de capaciteiten, intenties of activiteiten van buitenlandse organisaties die een actuele of potentiële bedreiging voor de nationale veiligheid van de VS of bondgenoten van de VS vormen; het begrijpen of beoordelen van transnationale dreigingen die van invloed zijn op de mondiale veiligheid, met inbegrip van risico's voor de volksgezondheid; en bescherming tegen transnationale criminele dreigingen[49].

In de derde plaats heeft de RISAA de definitie van "aanbieder van elektronische-communicatiediensten" uitgebreid, waardoor het aantal bedrijven die op grond van artikel 702 FISA kunnen worden verplicht om informatie te verstrekken, is verruimd[50]. De definitie omvat nu ook andere dienstverleners die "toegang hebben tot apparatuur die wordt of kan worden gebruikt om draadgebonden of elektronische communicatie te verzenden of op te slaan", terwijl openbare accommodaties, woningen, gemeenschapsvoorzieningen en horecagelegenheden uitdrukkelijk zijn uitgesloten. In een brief aan het Congres heeft het ministerie van Justitie deze wijziging beschreven als een technische wijziging die tot doel heeft om een "uiterst klein" aantal technologiebedrijven die volgens recente beslissingen van de FISC en de Foreign Intelligence Surveillance Court of Review (rechterlijke beroepsinstantie voor buitenlandse-inlichtingensurveillance van de VS) (FISCR) niet onder de vorige definitie vielen, binnen het

[47] Artikel 22 RISAA.
[48] Artikel 23 RISAA.
[49] Artikel 2, (b), (ii), (A), (2), (3) en (10), EO 14086.
[50] Artikel 25 RISAA.

toepassingsgebied ervan te brengen[51]. In diezelfde brief heeft het ministerie van Justitie toegezegd het toepassingsgebied te beperken door deze definitie uitsluitend toe te passen op het type dienstverlener dat aan de orde was in de gerechtelijke procedure die tot het FISC-besluit heeft geleid. Als gevolg hiervan worden de betrokken bedrijven genoemd in een gerubriceerde bijlage voor het Congres. Verschillende ngo's, waaronder die welke feedback hebben verstrekt in het kader van de evaluatie, hebben hun zorgen geuit over de uitbreiding, waarbij zij aanvoerden dat deze potentieel een groot aantal Amerikaanse bedrijven kan omvatten (aangezien vele daarvan enig type elektronische-communicatiedienst verlenen en toegang hebben tot communicatieapparatuur). In het licht van die zorgen is, met steun van de inlichtingendiensten, een nieuwe wijziging voorgesteld in de ontwerp-Intelligence Authorisation Act for Fiscal Year 2025 (machtigingswet betreffende inlichtingen voor het begrotingsjaar 2025), die momenteel in behandeling bij het Congres is. Deze wijziging, indien aangenomen door het Congres, zal ervoor zorgen dat alleen de bedrijven die in bovengenoemde beslissingen van de FISC worden genoemd nieuw onder de definitie van aanbieder van elektronische-communicatiediensten zullen komen te vallen. Het wetsvoorstel voorziet er ook in dat elk bevel dat tot een van die bedrijven is gericht, moet worden gemeld aan de FISC, zodat deze kan beoordelen of het betreffende bedrijf inderdaad binnen het toepassingsgebied van de definitie valt. In zijn brief aan het Congres heeft het ministerie van Justitie zich ertoe verbonden om elke zes maanden verslag uit te brengen aan het Congres over alle toepassingen van de bijgewerkte definitie, zodat het Congres het passende parlementaire toezicht kan uitoefenen op de enge toepassing van de definitie.

Belangrijk is dat tijdens de evaluatievergadering door de Amerikaanse autoriteiten en de PCLOB is bevestigd dat alle waarborgen van EO 14086 volledig van toepassing blijven op elke verzameling en elk het gebruik van gegevens uit hoofde van artikel 702 FISA, ook na deze wijzigingen. De RISAA breidt het aantal bedrijven dat een bevel kan krijgen enigszins uit, maar beperkt niet de uitoefening van rechten. Desalniettemin zal het belangrijk zijn om verdere ontwikkelingen (wetgeving en rapportage) nauwlettend te volgen en informatie over de praktische toepassing van deze nieuwe regels te verkrijgen. Daarbij gaat het bijvoorbeeld over de gevolgen van de verruiming van de definities van "buitenlandse inlichtingen" en "aanbieder van elektronische-communicatiediensten" voor het aantal doelwitten dat op grond van artikel 702 FISA wordt geselecteerd (zoals jaarlijks meegedeeld door het ODNI, zie hieronder met betrekking tot transparantie). Het toekomstige follow-upverslag van het recente PCLOB-verslag over artikel 702 FISA (zie hieronder) zou in dit opzicht zeer informatief moeten zijn.

Institutionele en procedurele wijzigingen

In het kader van de institutionele en procedurele wijzigingen heeft de RISAA diverse procedures die in de praktijk al werden gevolgd, gecodificeerd en nieuwe waarborgen ingevoerd. Hoewel sommige daarvan alleen betrekking hebben op Amerikaanse personen, verhogen verschillende wijzigingen de bescherming voor zowel Amerikaanse als niet-

[51] https://www.justice.gov/opa/media/1348621/dl?inline. Zie de beslissing van de FISC van 2022 (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) en de uitspraak van de FISCR waarin die beslissing wordt bevestigd (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

Amerikaanse personen van wie op grond van artikel 702 FISA gegevens kunnen worden verzameld[52], waardoor deze relevant zijn voor de werking van het DPF.

In de eerste plaats is een aantal aanvullende verantwoordings-, toezichts- en rapportagevereisten ingevoerd. In het bijzonder moet FBI-personeel nu jaarlijks een training volgen over de regels die van toepassing zijn op het doorzoeken van op grond van artikel 702 FISA verkregen informatie[53]. De FBI is ook verplicht om verslag over zijn zoekactiviteiten uit te brengen aan het Congres (bv. over het aantal zoekopdrachten dat is uitgevoerd met behulp van zogenoemde "batch job"-technologieën, waarbij meerdere zoektermen worden ingevoerd als onderdeel van één enkele zoekopdracht), evenals over de verantwoordingsmaatregelen die zijn genomen om de naleving van de wettelijke vereisten voor zoekactiviteiten te waarborgen (artikelen 11 en 12 RISAA). Bovendien heeft de inspecteur-generaal van het ministerie van Justitie instructies om een verslag over de naleving van de wettelijke vereisten voor zoekactiviteiten door de FBI op te stellen (artikel 9 RISAA). Meer in het algemeen zijn het ODNI en de minister van Justitie nu verplicht, teneinde de transparantie van de procedures voor de FISC te vergroten, om de beoordeling inzake de derubricering van door de FISC gegeven beslissingen binnen 180 dagen af te ronden (artikel 7 RISAA). Daarnaast moeten transcripties van alle hoorzittingen voor de FISC en de FISCR, waar beroep kan worden ingesteld tegen FISC-beslissingen, worden bewaard en toegezonden aan het Congres (artikel 8 RISAA).

In de tweede plaats heeft de RISAA verdere beperkingen ingevoerd op het gebruik van op grond van artikel 702 FISA verzamelde gegevens door de FBI. Artikel 2, (d), RISAA bepaalt dat een zoekopdracht met behulp van "batchtechnologie" alleen kan worden uitgevoerd na goedkeuring van de juridische dienst van de FBI, tenzij er sprake is van zeer dringende omstandigheden. Voorts is het voor de FBI nu verboden om automatische controles uit te voeren op niet-geminimaliseerde informatie die op grond van artikel 702 FISA is verkregen en moeten analisten van de FBI "affirmatief" (d.w.z. met een bevestiging) zoektermen selecteren. De RISAA verbiedt de FBI nu ook om zoekopdrachten uit te voeren die uitsluitend tot doel hebben om bewijs van criminele activiteiten te vinden en te extraheren (tenzij er een redelijke overtuiging bestaat dat die zoekopdrachten kunnen helpen bij het beperken of elimineren van een dreiging voor het leven of van ernstig lichamelijk letsel, of waar nodig om te voldoen aan openbaarmakingsverplichtingen in gerechtelijke procedures)[54]. Bovendien mag de FBI geen niet-geminimaliseerde gegevens opnemen in opslagplaatsen voor analytische gegevens, tenzij de persoon die het doelwit is relevant is voor een bestaand onderzoek met betrekking tot de nationale veiligheid[55].

[52] Daarnaast heeft de RISAA enkele wijzigingen ingevoerd met betrekking tot het traditionele geïndividualiseerd elektronisch toezicht op grond van artikel 105 FISA (op basis van een bevel dat de FISC uitvaardigt wanneer is aangetoond dat er sprake is van een "redelijk vermoeden"). Een verzoek van een inlichtingendienst om een bevel tot uitvoering van geïndividualiseerd elektronisch toezicht van de minister van Justitie vereist nu een beëdigde verklaring waarin wordt gerechtvaardigd dat is voldaan aan de voorwaarden van artikel 105 FISA (artikel 6, (a), RISAA). De mogelijke duur van elektronisch toezicht op buitenlandse mogendheden of agenten van buitenlandse mogendheden is verlengd van 120 dagen tot een jaar (artikel 6, (g), RISAA).

[53] Artikel 2, (d), RISAA.

[54] Artikel 3, (a), RISAA.

[55] Artikel 3, (b), RISAA. Indien noodzakelijk vanwege dringende omstandigheden kan de FBI-directeur een uitzondering op deze bepaling toestaan, waarvan kennisgeving moet worden gedaan aan het Congres.

In de derde plaats zijn enkele bepalingen betreffende de status en de rol van "amici curiae" voor de FISC gewijzigd[56]. De "amici" worden aangewezen als deskundigen om de FISC (en de FISCR) te ondersteunen in aangelegenheden die verband houden met privacy en burgerlijke vrijheden, of om technologische kwesties te helpen verduidelijken, in het kader van de behandeling van een specifieke aanvraag van een overheid. Terwijl de FISA voorheen vereiste dat "amici" beschikken over deskundigheid op het gebied van privacy en burgerlijke vrijheden, het verzamelen van inlichtingen, communicatietechnologie of andere relevante gebieden, bepaalt deze wet nu in beginsel dat zij deskundig moeten zijn op het gebied van privacy/burgerlijke vrijheden en het verzamelen van inlichtingen. De FISC had reeds de mogelijkheid om een "amicus" te benoemen in elke zaak waarin zij dat het passend achtten en was verplicht om dit te doen in geval van een nieuwe of belangrijke uitlegging van de wet. Na de hernieuwde goedkeuring is de FISC nu ook verplicht om bij elk verzoek om toestemming voor een FISA-certificering op grond van artikel 702 en de bijbehorende procedures (bv. procedures voor het specificeren van doelwitten) een "amicus" aan te stellen, tenzij hij van oordeel is dat dit niet passend is of waarschijnlijk tot onnodige vertraging zou leiden[57]. Bovendien kan de FISC nu besluiten om in plaats van één, een of meerdere "amici" te benoemen. Ook wordt verduidelijkt dat de door "amici" te verstrekken informatie "beperkt [moet] blijven tot specifieke door de rechter vastgestelde kwesties", hoewel de onderwerpen waarover "amici" opmerkingen kunnen maken (in de vorm van juridische argumenten en informatie inzake de bescherming van de privacy en de burgerlijke vrijheden van Amerikaanse personen, het verzamelen van inlichtingen en het gebruik van communicatietechnologie, naast andere relevante onderwerpen) een breed scala aan gebieden blijft bestrijken.

Ten slotte wordt in artikel 18 RISAA een "commissie voor de hervorming van de FISA" ingesteld — bestaande uit onder meer leden van het Congres, de voorzitter van de PCLOB, de eerste adjunct-directeur voor de nationale inlichtingendiensten (Principal Deputy Director of National Intelligence) en de plaatsvervangend minister van Justitie (Deputy Attorney General) en andere, door het Congres benoemde leden[58] —, die tot taak heeft om aanbevelingen te doen voor aanvullende FISA-hervormingen.

De Commissie zal de verdere ontwikkelingen met betrekking tot artikel 702 FISA nauwlettend volgen, onder meer in het kader van de toezichtsactiviteiten van de PCLOB (zie hieronder), de werkzaamheden van de hervormingscommissie en de komende herziening van de FISA na twee jaar.

2.2.1.3. Surveillanceactiviteiten in de praktijk: cijfers en trends

Uit het jaarlijkse statistische transparantieverslag van het ODNI over de gebruikmaking van de surveillanceautoriteiten op het gebied van nationale veiligheid door de inlichtingendiensten voor het kalenderjaar 2023 ("Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities for Calendar Year 2023"), dat in april 2024 is gepubliceerd[59], blijkt dat het aantal doelwitten uit hoofde van artikel 702 FISA is gestegen van 245 073 in het kalenderjaar 2022 tot 268 590 in het kalenderjaar 2023. In dat verslag wordt uitgelegd dat fluctuaties in het aantal doelwitten verschillende redenen kunnen hebben, waaronder wijzigingen in operationele prioriteiten,

[56] Voor de duidelijkheid: deze wijzigingen hebben geen invloed op de status en rol van de speciale advocaten voor de Data Protection Review Court (DPRC), zoals is bevestigd door de VS tijdens de evaluatievergadering.
[57] Artikel 5, (b), RISAA.
[58] Artikel 18 vereist uitdrukkelijk vertegenwoordiging van buiten het Congres.
[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

gebeurtenissen in de wereld, technische capaciteiten, gedrag van doelwitten en veranderingen in de telecommunicatiesector. In het verslag wordt ook vermeld dat geen enkele niet-Amerikaanse persoon (tegen 1 in 2021 en 0 in 2022) was aangewezen als doelwit overeenkomstig artikel 402 FISA ("pen register and trap and trace devices" (trackers van berichtenverkeer)), terwijl er zes bevelen (tegen 11 in zowel 2021 als 2022) in verband met zes doelwitten (tegen 13 in 2021 en 11 in 2022) waren uitgevaardigd overeenkomstig artikel 501 FISA (toegang tot bedrijfsdocumenten van algemene vervoerbedrijven, autoverhuurfaciliteiten en fysieke opslagfaciliteiten), waarbij 5 412 unieke identificatiecodes (tegen 23 157 in 2021 en 55 431 in 2022) waren gebruikt om krachtens die bevelen verzamelde informatie te communiceren.

Uit het jaarlijkse verslag van het ministerie van Justitie over de uitvoering van de FISA aan het Congres blijkt dat er in het kalenderjaar 2023 327 verzoeken om elektronisch toezicht en/of de uitvoering van fysieke zoekopdrachten voor het verkrijgen van buitenlandse inlichtingen op grond van respectievelijk artikel 105 en artikel 302 FISA[60] zijn ingediend bij de FISC. Het totale aantal personen dat als doelwit werd geselecteerd, lag tussen 500 en 999. Met betrekking tot de "national security letters" (bevelen tot verzameling van inlichtingen voor doeleinden van nationale veiligheid), wordt in het verslag vermeld dat er in 2023 (met uitsluiting van verzoeken om alleen abonneegegevens) 10 115 verzoeken om informatie over 3 033 verschillende niet-Amerikaanse personen zijn ingediend[61].

Verschillende DPF-gecertificeerde bedrijven (zoals Google, Meta) maken gebruik van de mogelijkheid die de Amerikaanse wetgeving biedt om transparantieverslagen te publiceren met informatie over het aantal verzoeken uit hoofde van de FISA en het aantal verzoeken om een national security letter die zij in een gegeven verslagperiode hebben ontvangen. Ten tijde van het opstellen van dit verslag waren de statistieken over het aantal verzoeken uit hoofde van de FISA na juli 2023 nog niet beschikbaar. Zo heeft Google bijvoorbeeld gerapporteerd dat zij in de periode juli-december 2023 500 tot 999 verzoeken om een national security letter had ontvangen, die betrekking hadden op 2 000 tot 2 499 accounts[62]. Meta meldde dat het in dezelfde verslagperiode 0 tot 499 verzoeken om een national security letter had ontvangen, die betrekking hadden op 500 tot 999 accounts[63]. De aantallen zijn de afgelopen jaren redelijk stabiel gebleven. Om de transparantie verder te vergroten, publiceren sommige bedrijven (zoals Google), nadat de geheimhoudingsbeperkingen zijn opgeheven, proactief informatie over het aantal national security letters die zij hebben ontvangen[64].

2.2.1.4. Andere ontwikkelingen

In het kader van de voorbereiding van de herziening hebben meerdere ngo's vragen gesteld over nieuwe vormen van gegevensverzameling door Amerikaanse inlichtingendiensten, zoals de aankoop van gegevens van commerciële entiteiten, met name gegevensmakelaars. Daarbij

[60] https://www.justice.gov/nsd/media/1350236/dl?inline.

[61] Deze cijfers zijn grosso modo gelijk gebleven ten opzichte van het voorgaande verslagjaar (2022). Ter vergelijking: in 2022 waren er 317 definitieve verzoeken voor het uitvoeren van elektronisch toezicht en/of fysieke zoekopdrachten ten behoeve van buitenlandse inlichtingen ingediend bij de FISC. Het totale aantal personen tegen wie een bevel tot elektronisch toezicht werd uitgevaardigd, lag tussen 0 en 499. De FBI heeft in 2022 9 103 verzoeken om een national security letter ingediend met het oog op de verkrijging van informatie over niet-Amerikaanse personen (met uitsluiting van verzoeken om alleen abonneegegevens). Bron: https://irp.fas.org/agency/doj/fisa/2022rept.pdf.

[62] https://transparencyreport.google.com/user-data/us-national-security.

[63] https://transparency.meta.com/reports/government-data-requests/country/US/.

[64] https://transparencyreport.google.com/user-data/us-national-security.

legden zij uit dat gegevens die op deze basis worden verzameld, weliswaar nog steeds moeten worden verwerkt in overeenstemming met andere vereisten, onder meer overeenkomstig EO 12333[65], maar dat die verwerving plaatsvindt buiten het kader van FISA en EO 14086.

In dit verband zij eraan herinnerd dat elke vorm van vrijwillig delen van gegevens met derden is onderworpen aan een aantal gedetailleerde voorwaarden overeenkomstig het DPF. In de eerste plaats kan een gecertificeerde organisatie geen gegevens delen met een derde partij (die niet optreedt als vertegenwoordiger/verwerker) zonder de betrokkene(n) daarvan in kennis te stellen en een keuzemogelijkheid voor te leggen[66]. In de tweede plaats kunnen verdere doorgiften volgens het "Accountibility for Onward Transfer Principle" (beginsel van verantwoording voor de verdere doorgifte) alleen plaatsvinden 1) voor beperkte en gespecificeerde doeleinden; 2) op basis van een overeenkomst tussen de EU-VS-DPF-organisatie en de derde; en 3) indien die overeenkomst de derde verplicht hetzelfde beschermingsniveau te bieden als het niveau dat wordt gewaarborgd door de beginselen[67].

Daarnaast heeft de FTC, zoals ook besproken tijdens de evaluatievergadering, handhavingsmaatregelen genomen tegen gegevensmakelaars die gevoelige consumentengegevens verkopen. Zo heeft de FTC in een zaak tegen X-Mode en zijn rechtsopvolger Outlogic dat bedrijf bij een bevel van 9 januari 2024 verboden om geolocatiegegevens aan derden te verkopen en opgedragen om onrechtmatig door het bedrijf gebruikte en gedeelde gegevens te verwijderen. Uit het onderzoek van de FTC was onder meer gebleken dat het bedrijf personen niet volledig had geïnformeerd over het gebruik en de verkoop van hun geolocatiegegevens, geen maatregelen had genomen om personen in staat te stellen zich te verzetten tegen tracking, het gebruik van gegevens voor mogelijk discriminerende doeleinden had toegestaan en geen beperkingen had gesteld aan het gebruik van de betreffende informatie door derden[68]. De Commissie verwacht dat de FTC dezelfde aanpak zal volgen wanneer DPF-gecertificeerde bedrijven in strijd met bovengenoemde bepalingen gegevens zouden delen.

Tot slot is het vermeldenswaard dat het ODNI in mei 2024 zijn beleidskader voor commercieel beschikbare informatie voor de inlichtingendiensten[69] heeft gepubliceerd. Dat beleidskader voorziet in een aantal beginselen en vereisten die inlichtingendiensten moeten volgen, onder meer om bij het verkrijgen en gebruiken van informatie in het kader van een commerciële transactie de risico's voor de privacy en de burgerlijke vrijheden tot een minimum te beperken.

2.2.2. Onafhankelijk toezicht

De activiteiten van Amerikaanse inlichtingendiensten staan onder toezicht van verschillende instanties, waaronder functionarissen voor privacy en burgerlijke vrijheden (Privacy and Civil Liberties Officers), inspecteurs-generaal, het Congres en de PCLOB. Met name vereist EO 14086 dat elke inlichtingendienst hoge functionarissen voor wetgeving, toezicht en

[65] Zie bijvoorbeeld artikel 2.4, EO 12333 inzake verzamelingstechnieken.
[66] Zie overweging 40 van het adequaatheidsbesluit.
[67] Zie overweging 38 van het adequaatheidsbesluit.
[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.
[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. Inlichtingendiensten moeten met ingang van augustus 2024 voldoen aan het kader.

naleving aanwijst om ervoor te zorgen dat de toepasselijke Amerikaanse wetgeving wordt nageleefd. Deze toezichtfunctie wordt vervuld door functionarissen met een aangewezen nalevingsfunctie en door functionarissen voor privacy en burgerlijke vrijheden en inspecteurs-generaal[70]. Zij moeten periodiek toezicht houden op SIGINT-activiteiten en ervoor zorgen dat alle gevallen van niet-naleving worden verholpen. De inlichtingendiensten moeten deze functionarissen toegang verlenen tot alle informatie die relevant is voor de uitvoering van hun toezichthoudende taken en mogen geen acties ondernemen om die toezichthoudende activiteiten te belemmeren of op ongepaste wijze te beïnvloeden.

De juridisch adviseur van het bureau van de inspecteur-generaal van de inlichtingendiensten (Intelligence Services Inspector General, "ICIG") van het ODNI — dat beschikt over ruime bevoegdheden jegens alle inlichtingendiensten, waaronder de bevoegdheid om klachten of informatie over vermeend onrechtmatig gedrag of misbruik van gezag te onderzoeken — heeft deelgenomen aan de evaluatievergadering. Daarin bevestigde hij dat het ICIG systematisch de naleving van EO 14086 controleert als onderdeel van zijn toezichtsactiviteiten. Ook verwees hij naar recente toezichtsactiviteiten van andere inspecteurs-generaal van de inlichtingendiensten, zoals beschreven in hun reguliere verslagen. Zo heeft de inspecteur-generaal van de NSA in zijn halfjaarlijkse verslag aan het Congres voor de periode april-september 2023[71] het Congres geïnformeerd over een evaluatie van een intern NSA-controlekader voor besluiten en verzoeken om het doelwit te specificeren ("targeting"). De inspecteur-generaal van de NSA concludeerde in zijn verslag dat het kader naar behoren functioneerde om de naleving van wetgeving, richtlijnen en beleidsmaatregelen ter bescherming van de burgerlijke vrijheden en de privacy te waarborgen. In hetzelfde rapport wordt ook melding gemaakt van een onderzoek waaruit naar voren was gekomen dat een NSA-medewerker een SIGINT-tool had misbruikt voor ongeoorloofde doeleinden.

Krachtens EO 14086[72] zijn specifieke toezichtstaken toevertrouwd aan de PCLOB[73]. De voorzitter van de PCLOB en de drie leden ervan hebben deelgenomen aan de evaluatievergadering en hebben daarin meegedeeld dat de PCLOB in april 2023 inlichtingendiensten had geadviseerd over hun ontwerpbeleid en -procedures ter uitvoering van

[70] Elke inlichtingendienst heeft een inspecteur-generaal die wettelijk onafhankelijk is en verantwoordelijk is voor het uitvoeren van audits en onderzoeken met betrekking tot de activiteiten die door de desbetreffende dienst worden uitgevoerd ten behoeve van de nationale veiligheid. Zij hebben toegang tot al het relevante (met inbegrip van gerubriceerd) materiaal, indien nodig door middel van een dwangbevel, en kunnen getuigenverklaringen afleggen. De inspecteurs-generaal verwijzen gevallen van vermoedelijke strafbare feiten door voor vervolging en doen aanbevelingen voor corrigerende maatregelen aan het hoofd van hun dienst. Hoewel hun aanbevelingen niet-bindend zijn, worden hun verslagen, waaronder die over follow-upmaatregelen (of het ontbreken daarvan) doorgaans openbaar gemaakt en aan het Congres toegezonden. Zie in dit verband voetnoot 136 van het adequaatheidsbesluit over de rol van de inspecteur-generaal.

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

[72] De PCLOB is een onafhankelijk orgaan met verantwoordelijkheden op het gebied van terrorismebestrijdingsbeleid en de uitvoering daarvan met het oog op de bescherming van de privacy en de burgerlijke vrijheden. De PCLOB heeft toegang tot alle relevante (inclusief gerubriceerde) informatie, kan gesprekken voeren en kan getuigen horen. Ook kan de PCLOB aanbevelingen doen aan rechtshandhavings- en inlichtingendiensten en rapporteert hij regelmatig aan het Congres en de president. De verslagen van de PCLOB worden voor zover mogelijk openbaar gemaakt.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

EO 14086 en was geraadpleegd over de benoeming van rechters en speciale advocaten van de Data Protection Review Court (toetsingsinstantie voor gegevensbescherming) (DPRC). Ook is de PCLOB gestart met een toezichtsproject om 1) de uitvoering van de door inlichtingendiensten aangenomen geactualiseerde beleidslijnen en procedures te beoordelen om te waarborgen dat deze in overeenstemming zijn met de Executive Order, en 2) een jaarlijkse beoordeling van de werking van het nieuwe verhaalsmechanisme uit te voeren (zie hieronder)[74]. De PCLOB-leden bevestigden dat de PCLOB voornemens is om beide beoordelingen in de nabije toekomst uit te voeren. Met betrekking tot het verhaalsmechanisme legden zij uit dat, bij gebreke van klachten, de beoordeling van de PCLOB gericht zal zijn op de beleidslijnen en procedures die zijn ingevoerd om het mechanisme op te zetten.

Wat andere toezichtsactiviteiten betreft, heeft de PCLOB op 28 september 2023 een verslag over artikel 702 FISA[75] uitgebracht. Dat verslag is een vervolg op een eerder verslag van 2014 en bevat geactualiseerde feitelijke en juridische informatie over de werking van -surveillanceprogramma's uit hoofde van artikel 702 FISA. Het verslag bevat ook aanbevelingen inzake de naleving van de toepasselijke vereisten door inlichtingendiensten en suggesties aan het Congres om verschillende aspecten van artikel 702 FISA verder te versterken in het kader van de hernieuwde goedkeuring (onder meer door het codificeren van de legitieme doelstellingen voor surveillanceactiviteiten zoals vermeld in EO 14086)[76]. Tijdens de evaluatievergadering heeft de PCLOB verklaard binnenkort antwoorden van inlichtingendiensten te verwachten over de uitvoering van zijn aanbevelingen, die vervolgens in aanmerking zullen worden genomen in een toekomstig follow-upverslag. Andere lopende toezichtsprojecten betreffen de bestrijding van binnenlands terrorisme en de impact daarvan op de privacy en de burgerlijke vrijheden, en het verzamelen van open-source- of commercieel beschikbare gegevens door de FBI[77].

Ten slotte hebben ngo's die in het kader van de evaluatie zijn geraadpleegd, zorgen geuit over het feit dat de ambtstermijn van verschillende PCLOB-leden in de nabije toekomst zal aflopen, waardoor de PCLOB mogelijk zonder quorum zal komen te zitten. Meer bepaald is de ambtstermijn van de voorzitter verstreken en eindigt de periode waarin zij in een tijdelijke hoedanigheid kan dienen in januari 2025, terwijl er nog een zetel vacant is en een derde zetel eveneens in januari volgend jaar vacant zal worden. Tijdens de evaluatievergadering hebben de leden uitgelegd dat zij niet verwachten dat de PCLOB zonder quorum zal komen te zitten, aangezien er al een voordracht is gedaan (die nog door de Senaat moet worden bekrachtigd) voor de zetel die momenteel vacant is[78]. De ngo's onderstreepten ook dat zelfs indien de PCLOB zijn quorum zou verliezen, dit geen invloed zou hebben op zijn vermogen om toezichtsprojecten te blijven uitvoeren. Gezien de belangrijke rol van de PCLOB bij de evaluatie van de uitvoering van EO 14086 zal de Commissie de status van toekomstige vacatures en voordrachten/benoemingen evenwel nauwlettend in het oog houden.

---

[74] https://www.pclob.gov/OversightProjects/Details/1115.

[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

[76] De Commissie merkt op dat enkele van die aanbevelingen zijn opgenomen in de RISAA, waaronder de aanbeveling inzake het verzamelen van "abouts" en de aanbeveling inzake het versterken van de rol van de FISC-deskundigen (amici).

[77] https://www.pclob.gov/OversightProjects.

[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.

2.2.3. Verhaalsmechanismen

EO 14086, aangevuld door een verordening van de minister van Justitie, heeft een nieuw verhaalsmechanisme ingesteld voor de behandeling en beslechting van in aanmerking komende klachten van personen in verband met Amerikaanse SIGINT-activiteiten[79]. Iedere natuurlijke persoon in de EU heeft het recht om bij het verhaalsmechanisme een klacht in te dienen over een vermeende schending van de Amerikaanse wetgeving inzake SIGINT-activiteiten (bv. EO 14086, artikel 702 FISA, EO 12333) die zijn of haar belangen op het gebied van privacy en burgerlijke vrijheden schaadt. Natuurlijke personen kunnen een klacht indienen bij een gegevensbeschermingsautoriteit in een EU-lidstaat, die de klacht via het secretariaat van de EDPB zal doorsturen naar het verhaalsmechanisme. Het mechanisme bestaat uit twee lagen, waarbij het eerste onderzoek van klachten wordt uitgevoerd door het CLPO van het ODNI en betrokkenen de mogelijkheid hebben om tegen het besluit van het CLPO op te komen bij de onafhankelijk DPRC. Zodra het onderzoek is afgerond, stelt de CLPO van het ODNI de klager er via de nationale autoriteit van in kennis dat "het onderzoek geen onder EO 14086 vallende schendingen aan het licht heeft gebracht of de CLPO van het ODNI/de DPRC een beslissing heeft gegeven die passende herstelmaatregelen vereist". De beslissingen van de CLPO van het ODNI en de DPRC hebben bindende kracht voor de inlichtingendiensten.

Sinds de vaststelling van het adequaatheidsbesluit zijn verdere stappen ondernomen om het verhaalsmechanisme volledig operationeel te maken.

In verband met de oprichting van de DPRC zijn op 14 november 2023 acht rechters benoemd (d.w.z. twee meer dan het minimumaantal dat wordt vereist door EO 14086, zoals aangevuld door regelgeving van de minister van Justitie (28 CFR § 201.3, (a))[80]. De rechters zijn benoemd op basis van de criteria van EO 14086 en volgens de daarin vastgestelde procedure, na raadpleging van onder andere de PCLOB[81]. Onder hen zijn voormalige rechters van federale districtsrechtbanken en hoven van beroep, een voormalige minister van Justitie en een voormalig lid van de PCLOB. Zoals vereist door de EO, heeft ten minste de helft van de rechters justitiële ervaring. Daarnaast zijn in april 2024 twee speciale advocaten — beoefenaars van juridische beroepen met deskundigheid op het gebied van zowel gegevensbescherming als nationale veiligheid — benoemd om de belangen van betrokkenen te vertegenwoordigen voor de DPRC. Tijdens de evaluatievergadering is bevestigd dat alle rechters en speciale advocaten de hoogste veiligheidsmachtiging hebben gekregen en derhalve toegang hebben tot gerubriceerd materiaal bij de uitvoering van hun taken voor de DPRC. De DPRC heeft ook een reeks veelgestelde vragen gepubliceerd met meer informatie over zijn rol, onafhankelijkheid en werking[82].

Wat de behandeling van klachten betreft, heeft het ODNI op 6 december 2022 Intelligence Community Directive 126 (richtlijn 126 inzake de inlichtingendiensten) vastgesteld, die verschillende aspecten van het onderzoek en de behandeling van klachten op gedetailleerde wijze regelt (door de vaststelling van termijnen, het opzetten van een beveiligd elektronisch register en beveiligde communicatiekanalen, het opleggen van een verplichting voor de CLPO en onderdelen van de inlichtingendiensten om in het kader van de jaarlijkse evaluatie van het

[79] Overwegingen 176 tot en met 194 van het adequaatheidsbesluit.
[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Artikel 3, (d), (A), EO 14086.
[82] https://www.justice.gov/opcl/dprc-resources.

verhaalsmechanisme samen te werken met de PCLOB enz.)[83]. Deze richtlijn is van toepassing op alle Amerikaanse inlichtingendiensten en is aangevuld met door individuele inlichtingendiensten vastgestelde interne procedures voor hun samenwerking met de CLPO van het ODNI in het kader van de behandeling van klachten (waarbij het bijvoorbeeld gaat om de ontwikkeling van een beveiligd register voor het delen van klachten en responsen daarop, en beveiligde communicatie tussen de betrokken instanties). Ook zal de DPRC in de komende maanden nadere regels voor de behandeling van klachten en andere procedurele aspecten uitvaardigen.

Zowel in de Europese Unie als in de VS is een aantal aanvullende maatregelen genomen om het algemene publiek te informeren en de indiening en afhandeling van klachten te vergemakkelijken. Voorbeelden daarvan zijn de goedkeuring door de EDPB van een informatieve nota over het nieuwe verhaalsmechanisme[84], een template voor een klachtenformulier (waarvan het de bedoeling is dat het door alle gegevensbeschermingsautoriteiten wordt vertaald en gepubliceerd in hun nationale ta(a)l(en))[85], en procedurevoorschriften die de samenwerking tussen nationale toezichthoudende autoriteiten en het secretariaat van de EDPB regelen[86]. Voorts heeft het ODNI een document met veelgestelde vragen en een factsheet over het nieuwe verhaalsmechanisme gepubliceerd en ontplooit het bewustmakingsactiviteiten voor het publiek[87].

Voorts hebben de EDPB en de betrokken Amerikaanse autoriteiten het afgelopen jaar nauw samengewerkt op verschillende operationele gebieden. Zoals tijdens de evaluatievergadering is bevestigd, hebben zij met name een versleuteld communicatiekanaal opgezet voor het doorsturen van klachten door nationale autoriteiten in de EU naar het secretariaat van de EDPB, door het secretariaat van de EDPB naar de CLPO van het ODNI en naar het bureau voor privacy en burgerlijke vrijheden (Office of Privacy and Civil Liberties, “OPCL”) van het ministerie van Justitie, en tussen de CLPO van het ODNI en andere autoriteiten aan Amerikaanse zijde (bv. de DPRC). Daarnaast heeft de CLPO van het ODNI toegelicht dat er nieuwe interne procedures zijn ingevoerd voor de samenwerking van individuele inlichtingendiensten met de CLPO van het ODNI bij de behandeling van klachten.

Tot slot heeft het OPCL, dat administratieve ondersteuning verleent aan de DPRC, ook meegedeeld dat de DPRC een eigen specifieke begrotingslijn heeft en beschikt over de benodigde faciliteiten om zijn taken uit te voeren, met inbegrip van beveiligde computers en laptops, telefoons enz. Zoals vereist door EO 14086, heeft het ministerie van Handel bovendien de nodige maatregelen genomen met het oog op het bijhouden van een register van alle ontvankelijke klachten die zijn ontvangen, waaronder het opzetten van een versleuteld communicatiekanaal met de CLPO van het ODNI. Het ministerie van Handel zal periodiek contact met de CLPO van het ODNI opnemen om te vragen of informatie met betrekking tot

[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.

[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_en.

[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_en.

[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_en.

[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf en https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

een individuele klacht is gederubriceerd. Indien dat het geval is, zal het ministerie van Handel de betrokken persoon daarvan in kennis stellen, zodat hij of zij inzage in die informatie kan verkrijgen.

Ten tijde van de evaluatievergadering waren er geen klachten van de toezichthoudende autoriteiten van de EU ontvangen en was het nieuwe verhaalsmechanisme daarom nog niet ingeroepen.

3. CONCLUSIE

Op basis van de informatie die voor deze eerste evaluatie is verzameld, concludeert de Commissie dat de Amerikaanse autoriteiten de benodigde structuren en procedures hebben ingevoerd om te waarborgen dat het kader voor gegevensbescherming effectief functioneert. In dit verband hecht de Commissie grote waarde aan de bijzonder goede samenwerking met de Amerikaanse autoriteiten bij het uitvoeren van de evaluatie.

In deze eerste evaluatie ligt de focus logischerwijs op de vraag of alle elementen van het kader zijn uitgevoerd, daar de ervaringen met de praktische toepassing van de waarborgen die van toepassing zijn op zowel de verwerking van gegevens door gecertificeerde bedrijven als de toegang tot gegevens door overheidsinstanties na slechts één jaar van werking van het kader vanzelfsprekend beperkt zijn. De Commissie zal de ontwikkelingen op dit gebied in de komende maanden en jaren dan ook nauwlettend volgen, met bijzondere aandacht voor 1) de komende verslagen van de PCLOB over de uitvoering van EO 14086 en de werking van het SIGINT-verhaalsmechanisme, en met name de werking van de DPRC; 2) mogelijke nieuwe wijzigingen van artikel 702 FISA; en 3) de voordracht en benoeming van leden van de PCLOB om toekomstige vacatures in te vullen.

Om een voortdurende en doeltreffende werking van het kader te waarborgen, acht de Commissie het daarenboven belangrijk dat:

- het ministerie van Handel van de VS, zoals aangekondigd tijdens de evaluatievergadering, intensiever gebruikmaakt van de verschillende instrumenten waarin het DPF voorziet voor het toezicht op de naleving van de beginselen door bedrijven en voor het opsporen van valse claims over deelname;
- de FTC haar proactieve aanpak van het onderzoeken en handhaven van de naleving van de DPF-beginselen door gecertificeerde bedrijven verder ontwikkelt; en
- het ministerie van Handel van de VS, de FTC en de gegevensbeschermingsautoriteiten van de EU gemeenschappelijke richtsnoeren inzake de belangrijkste vereisten uit hoofde van de DPF-beginselen ontwikkelen, zoals voor personeelsgegevens en verdere doorgiften.

In het licht van deze bevindingen van de evaluatie en in overeenstemming met overweging 211 van het adequaatheidsbesluit acht de Commissie het passend om de volgende periodieke evaluatie na drie jaar uit te voeren. Dit zou de ruimte moeten bieden om meer ervaring op te doen met de praktische toepassing van het DPF en om bovengenoemde toekomstige ontwikkelingen in aanmerking te nemen. De Commissie zal daarom, overeenkomstig artikel 3, lid 4, van het adequaatheidsbesluit, de EDPB en het bij artikel 93, lid 1, van de algemene

verordening gegevensbescherming (AVG) ingestelde comité raadplegen over de periodiciteit van toekomstige evaluaties.