UITVOERINGSBESLUIT (EU) 2023/1795 VAN DE COMMISSIE

van 10 juli 2023

overeenkomstig 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

(Kennisgeving geschied onder nummer C(2023) 4745)

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) ([1]), en met name artikel 45, lid 3,

Overwegende hetgeen volgt:

1. INLEIDING

(1) Bij Verordening (EU) 2016/679 ([2]) zijn de voorschriften vastgesteld voor de doorgifte van persoonsgegevens door verwerkingsverantwoordelijken of verwerkers in de Unie aan derde landen en internationale organisaties, voor zover die doorgiften onder het toepassingsgebied ervan vallen. De voorschriften inzake de internationale doorgifte van gegevens zijn vastgelegd in hoofdstuk V van die verordening. Hoewel het verkeer van persoonsgegevens van en naar landen buiten de Europese Unie noodzakelijk is voor de ontwikkeling van het grensoverschrijdende handelsverkeer en de internationale samenwerking, mogen doorgiften aan derde landen of internationale organisaties ([3]) niet ten koste gaan van het beschermingsniveau van de persoonsgegevens in de Unie.

(2) Op grond van artikel 45, lid 3, van Verordening (EU) 2016/679 kan de Commissie door middel van een uitvoeringshandeling besluiten dat een derde land, een gebied of één of meerdere nader bepaalde sectoren in een derde land een passend beschermingsniveau waarborgt. Onder deze voorwaarde kan de doorgifte van persoonsgegevens aan een derde land plaatsvinden zonder dat verdere toestemming noodzakelijk is, zoals bepaald in artikel 45, lid 1, en overweging 103 van Verordening (EU) 2016/679.

(3) Zoals bepaald in artikel 45, lid 2, van Verordening (EU) 2016/679 moet de vaststelling van een adequaatheidsbesluit berusten op een grondige analyse van de rechtsorde van het derde land, die zowel de voorschriften betreft die gelden voor de importeurs van gegevens als de beperkingen en waarborgen wat betreft de toegang van overheidsinstanties tot persoonsgegevens. Bij haar beoordeling moet de Commissie nagaan of het betrokken derde land een beschermingsniveau waarborgt dat "in feite overeenkomend" is met het niveau dat in de Unie wordt verzekerd (overweging 104 van Verordening (EU) 2016/679). Of dit het geval is, moet worden beoordeeld aan de hand van de wetgeving van de Unie, met name Verordening (EU) 2016/679, alsook de rechtspraak van het Hof van de Europese Unie (hierna "het Hof" genoemd) ([4]).

([1]) PB L 119 van 4.5.2016, blz. 1.
([2]) Voor de duidelijkheid werd een lijst met in dit besluit gebruikte afkortingen opgenomen in bijlage VIII.
([3]) Zie overweging 101 van Verordening (EU) 2016/679.
([4]) Zie de meest recente zaak, C-311/18, Facebook Ireland en Schrems (hierna "Schrems II" genoemd), ECLI:EU:C:2020:559.

(4) Zoals het Hof in zijn arrest van 6 oktober 2015 in zaak C-362/14, Maximillian Schrems/Data Protection Commissioner ([5]) ("Schrems"), heeft verduidelijkt, is het hiervoor niet noodzakelijk dat hetzelfde beschermingsniveau wordt geboden. Met name mogen de middelen die het derde land in kwestie voor de bescherming van de persoonsgegevens tot zijn beschikking heeft, anders zijn dan de middelen die binnen de Unie worden ingezet, zolang zij in de praktijk doeltreffend genoeg blijken om een passend beschermingsniveau te bieden ([6]). De adequaatheidsnorm vereist daarom niet dat de voorschriften van de Unie integraal worden overgenomen. Het gaat er veeleer om of het betreffende buitenlandse systeem als geheel het vereiste beschermingsniveau biedt, door de invulling van het recht op privacy, de doeltreffende toepassing en afdwingbaarheid daarvan en het toezicht dat wordt uitgeoefend ([7]). Voorts moet de Commissie volgens dit arrest bij de toepassing van deze norm met name beoordelen of het rechtskader van het betrokken derde land voorziet in regels ter beperking van inmengingen in de grondrechten van de personen van wie de gegevens vanuit de Unie worden doorgegeven, waarbij geldt dat de overheidsinstanties van dat land tot een dergelijke inmenging mogen overgegaan wanneer zij legitieme doelstellingen, zoals de nationale veiligheid, nastreven, en er effectieve rechtsbescherming tegen dat soort inmengingen bestaat ([8]). De adequaatheidsreferentie van het Europees Comité voor gegevensbescherming, die deze norm verder beoogt te verduidelijken, biedt in dit verband ook een leidraad ([9]).

(5) De toepasselijke norm met betrekking tot een dergelijke inmenging in de grondrechten op privacy en gegevensbescherming werd verder verduidelijkt door het Hof in zijn arrest van 16 juli 2020 in zaak C-311/18, Data Protection Commissioner/Facebook Ireland Limited en Maximillian Schrems (hierna "Schrems II"), waarbij Uitvoeringsbesluit (EU) 2016/1250 ([10]) van de Commissie inzake een eerder trans-Atlantisch kader voor gegevensstromen, het EU-VS-privacyschild (hierna "privacyschild" genoemd), nietig werd verklaard. Het Hof was van oordeel dat de beperkingen van de bescherming van persoonsgegevens die voortvloeien uit het interne recht van de Verenigde Staten inzake de toegang tot en het gebruik door de Amerikaanse overheidsinstanties van dergelijke gegevens die vanuit de Unie naar de Verenigde Staten worden doorgegeven, niet zodanig zijn afgebakend dat wordt voldaan aan vereisten die in grote lijnen overeenkomen met die welke in het Unierecht worden gesteld, wat de noodzaak en de evenredigheid van dergelijke inbreuken op het recht op gegevensbescherming betreft ([11]). Het Hof was ook van oordeel dat er geen rechtsmiddel bij een orgaan beschikbaar was dat personen wier gegevens aan de Verenigde Staten zijn doorgegeven, waarborgen biedt die in grote lijnen overeenkomen met die welke door artikel 47 van het Handvest betreffende het recht op een doeltreffende voorziening in rechte worden vereist ([12]).

(6) Na het arrest Schrems II is de Commissie besprekingen aangegaan met de Amerikaanse overheid met het oog op een mogelijk nieuw adequaatheidsbesluit dat zou voldoen aan de vereisten van artikel 45, lid 2, van Verordening (EU) 2016/679, zoals uitgelegd door het Hof. Als gevolg van deze besprekingen hebben de Verenigde Staten op 7 oktober 2022 uitvoeringsbevel (*Executive Order*) 14086 "Enhancing Safeguards for US Signals Intelligence Activities" [De waarborgen verbeteren voor activiteiten van de VS op het gebied van signals intelligence (SIGINT — inlichtingen uit het berichtenverkeer)] (EO 14086) vastgesteld, dat wordt aangevuld met een "Regulation on the Data Protection Review Court" (Verordening inzake de toetsingsinstantie voor gegevensbescherming), uitgevaardigd door de U.S. Attorney General (minister van Justitie van de Verenigde Staten) (hierna de "AG Regulation" genoemd) ([13]). Bovendien is het kader dat van toepassing is op commerciële entiteiten die gegevens verwerken die uit de Unie zijn doorgegeven in het kader van dit besluit — het "EU-VS-kader voor gegevensbescherming" (hierna het "EU-VS-DPF" of het "DPF" genoemd) — geactualiseerd.

(7) De Commissie heeft de Amerikaanse wetten en praktijken zorgvuldig geanalyseerd, met inbegrip van EO 14086 en de AG Regulation. Op basis van de bevindingen in de overwegingen 9 tot en met 200 concludeert de Commissie dat door de Verenigde Staten een passend beschermingsniveau wordt gewaarborgd voor persoonsgegevens die in het kader van het EU-VS-DPF door een verwerkingsverantwoordelijke of verwerker in de Unie ([14]) worden doorgegeven aan gecertificeerde organisaties in de Verenigde Staten.

([5]) Zaak C-362/14, Maximillian Schrems/Data Protection Commissioner (hierna "Schrems" genoemd), ECLI:EU:C:2015:650, punt 73.

([6]) Schrems, punt 74.

([7]) Zie de mededeling van de Commissie aan het Europees Parlement en de Raad "Uitwisseling en bescherming van persoonsgegevens in een geglobaliseerde wereld" (COM(2017) 7 final van 10.1.2017, punt 3.1, blz. 6-7).

([8]) Schrems, punten 88-89.

([9]) Europees Comité voor gegevensbescherming, Adequaatheidsreferentie, WP 254 rev. 01., beschikbaar op: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

([10]) Uitvoeringsbesluit (EU) 2016/1250 van de Commissie van 12 juli 2016 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de gepastheid van de door het EU-VS-privacyschild geboden bescherming (PB L 207 van 1.8.2016, blz. 1).

([11]) Schrems II, punt 185.

([12]) Schrems II, punt 197.

([13]) 28 CFR Part 302.

([14]) Dit besluit geldt voor de EER. De Overeenkomst betreffende de Europese Economische Ruimte (EER-overeenkomst) voorziet in de uitbreiding van de interne markt van de Europese Unie met de drie EER-staten IJsland, Liechtenstein en Noorwegen. Het besluit van het Gemengd Comité van de EER waarbij Verordening (EU) 2016/679 in bijlage XI bij de EER-overeenkomst wordt opgenomen, is vastgesteld door het Gemengd Comité van de EER op 6 juli 2018 en in werking getreden op 20 juli 2018. De verordening valt derhalve onder die overeenkomst. In het kader van het besluit moeten verwijzingen naar de EU en de lidstaten van de EU derhalve worden begrepen als verwijzingen die ook betrekking hebben op de EER-staten.

(8) Dit besluit heeft tot gevolg dat doorgifte door verwerkingsverantwoordelijken en verwerkers in de Unie ([15]) aan gecertificeerde organisaties in de Verenigde Staten zonder verdere toestemming kan plaatsvinden. Dit doet geen afbreuk aan de directe toepassing van Verordening (EU) 2016/679 op dergelijke entiteiten, voor zover is voldaan aan de voorwaarden betreffende het territoriale toepassingsgebied zoals vastgelegd in artikel 3 van die verordening.

2. HET EU-VS-KADER VOOR GEGEVENSBESCHERMING

2.1 Persoonlijk en materieel toepassingsgebied

2.1.1 *Gecertificeerde organisaties*

(9) Het EU-VS-DPF is gebaseerd op een systeem van certificering waarbij Amerikaanse organisaties een reeks privacybeginselen onderschrijven — de beginselen van het EU-VS-kader voor gegevensbescherming, met inbegrip van de aanvullende beginselen (hierna samen "de beginselen" genoemd) — die door het Amerikaanse ministerie van Handel (*U.S. Department of Commerce*) zijn gepubliceerd en in bijlage I bij dit besluit zijn opgenomen ([16]). Om in aanmerking te komen voor certificering krachtens het EU-VS-DPF moet een organisatie onderworpen zijn aan de onderzoeks- en handhavingsbevoegdheden van de Federal Trade Commission (FTC) of het Amerikaanse ministerie van Vervoer (*U.S. Department of Transportation*) ([17]). De beginselen zijn onmiddellijk na de certificering van toepassing. Zoals in de overwegingen 48 tot en met 52 nader wordt toegelicht, moeten de EU-VS-DPF-organisaties jaarlijks opnieuw certificeren dat zij de beginselen onderschrijven ([18]).

2.1.2 *Definities van persoonsgegevens en de concepten van verwerkingsverantwoordelijke en "vertegenwoordiger"*

(10) De bescherming die het EU-VS-DPF biedt, geldt voor alle persoonsgegevens die vanuit de Unie worden doorgegeven aan organisaties in de VS die bij het ministerie van Handel hebben gecertificeerd dat zij de beginselen onderschrijven, met uitzondering van gegevens die worden verzameld voor publicatie, uitzending of andere vormen van openbare communicatie van journalistiek materiaal en informatie in eerder gepubliceerd materiaal dat uit media-archieven wordt verspreid ([19]). Deze informatie kan derhalve niet worden doorgegeven op basis van het EU-VS-DPF.

(11) De beginselen definiëren persoonsgegevens/persoonlijke informatie op dezelfde manier als Verordening (EU) 2016/679, d.w.z. als "gegevens over een geïdentificeerde of identificeerbare persoon die binnen het toepassingsgebied van de AVG vallen en door een organisatie in de Verenigde Staten uit de EU zijn ontvangen en in welke vorm dan ook zijn vastgelegd" ([20]). Bijgevolg hebben zij ook betrekking op gepseudonimiseerde (of "versleutelde") onderzoeksgegevens (ook wanneer de sleutel niet wordt gedeeld met de ontvangende Amerikaanse organisatie) ([21]). Evenzo wordt het begrip verwerking gedefinieerd als "elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken of verspreiden, alsmede het wissen of vernietigen van gegevens" ([22]).

(12) Het EU-VS-DPF is van toepassing op organisaties in de VS die als verwerkingsverantwoordelijke (d.w.z. als een persoon of organisatie die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt) ([23]) of verwerker (d.w.z. een vertegenwoordiger die namens een verwerkingsverantwoordelijke optreedt) ([24]) worden aangemerkt. Amerikaanse verwerkers moeten er contractueel toe verbonden zijn dat zij slechts volgens instructies van de EU-verwerkingsverantwoordelijke handelen en die laatste bijstaan bij het

([15]) Dit besluit laat de vereisten van Verordening (EU) 2016/679 die van toepassing zijn op de entiteiten (verwerkingsverantwoordelijken en verwerkers) in de Unie die de gegevens doorgeven, bijvoorbeeld inzake doelbinding, minimale verwerking van gegevens, transparantie en gegevensbeveiliging, onverlet (zie ook artikel 44 van Verordening (EU) 2016/679).

([16]) Zie in dit verband Schrems, punt 81, waarin het Hof heeft bevestigd dat een systeem van zelfcertificering een passend beschermingsniveau kan waarborgen.

([17]) Bijlage I, hoofdstuk I, punt 2. De FTC heeft ruime rechtsbevoegdheid ten aanzien van commerciële activiteiten, met enkele uitzonderingen, bv. met betrekking tot banken, luchtvaartmaatschappijen, het verzekeringswezen en de niet-private transmissieactiviteiten van dienstverleners in de telecommunicatie (hoewel het U.S. Court of Appeals for the Ninth Circuit van 26 februari 2018 in zijn beslissing in de zaak FTC/AT&T heeft bevestigd dat de FTC rechtsbevoegdheid heeft over de private transmissieactivietien van dergelijke entiteiten). Zie ook voetnoot 2 van bijlage IV. Het ministerie van Vervoer is bevoegd om de naleving door luchtvaartmaatschappijen en reisbureaus (voor luchtvervoer) te handhaven, zie bijlage V, deel A.

([18]) Bijlage I, hoofdstuk III, punt 6.

([19]) Bijlage I, hoofdstuk III, punt 2.

([20]) Bijlage I, hoofdstuk I, punt 8, a).

([21]) Bijlage I, hoofdstuk III, punt 14, g).

([22]) Bijlage I, hoofdstuk I, punt 8, b).

([23]) Bijlage I, hoofdstuk I, punt 8, c).

([24]) Zie bv. bijlage I, hoofdstuk II, punt 2, b), punt 3, b) en punt 7, d), waaruit duidelijk blijkt dat vertegenwoordigers namens een verwerkingsverantwoordelijke optreden, op grond van de instructies van die laatste en volgens specifieke contractuele verplichtingen.

geven van antwoord aan natuurlijke personen die hun rechten uit hoofde van de beginselen uitoefenen ([25]). In het geval van subverwerking moet de verwerker bovendien een overeenkomst met de subverwerker sluiten die hetzelfde beschermingsniveau garandeert als de beginselen, en stappen ondernemen om voor de correcte uitvoering daarvan te zorgen ([26]).

2.2 **Beginselen van het EU-VS-kader voor gegevensbescherming**

2.2.1 ***Doelbinding en keuze***

(13) Persoonsgegevens moeten op rechtmatige en behoorlijke wijze worden verwerkt. Persoonsgegevens moeten worden verzameld voor een specifiek doel en mogen vervolgens uitsluitend worden gebruikt voor doeleinden die niet onverenigbaar zijn met het doel van de verwerking.

(14) Onder het EU-VS-DPF wordt dit gewaarborgd via verschillende beginselen. Ten eerste mag een organisatie onder het *Data Integrity and Purpose Limitation Principle* (beginsel van gegevensintegriteit en doelbinding), vergelijkbaar met artikel 5, lid 1, punt b), van Verordening (EU) 2016/679, geen persoonsgegevens verwerken op een wijze die onverenigbaar is met het doel waarvoor deze oorspronkelijk zijn verzameld of waarvoor de betrokkene later toestemming heeft gegeven ([27]).

(15) Ten tweede moet de organisatie, voordat zij persoonsgegevens gebruikt voor een nieuw (gewijzigd) doel dat wezenlijk verschilt maar nog steeds verenigbaar is met het oorspronkelijke doel, of voordat zij deze aan derden verstrekt, de betrokkenen de mogelijkheid bieden om bezwaar te maken (opt-out), overeenkomstig het *Choice Principle* (keuzebeginsel) ([28]), door middel van een duidelijk, opvallend en gemakkelijk beschikbaar mechanisme. Belangrijk is dat dit beginsel niet in de plaats treedt van het uitdrukkelijke verbod op onverenigbare verwerking ([29]).

([25]) Bijlage I, hoofdstuk III, punt 10, a). Zie ook de richtsnoeren die door het ministerie van Handel, in overleg met Europees Comité voor gegevensbescherming, zijn opgesteld in het kader van het privacyschild, waarin werd verduidelijkt aan welke verplichtingen Amerikaanse verwerkers die persoonsgegevens uit de Unie ontvangen in dat kader moeten voldoen. Aangezien deze regels niet gewijzigd zijn, blijven deze richtsnoeren/FAQ geldig voor het EU-VS-DPF (https://www.privacyshield.gov/article?id=Processing-FAQs).

([26]) Bijlage I, hoofdstuk II, punt 3, b).

([27]) Bijlage I, hoofdstuk II, punt 5, a). Verenigbare doelen kunnen onder meer auditing, fraudepreventie of andere doeleinden zijn die in overeenstemming zijn met de verwachtingen van een redelijk persoon gezien de context van de verzameling (zie bijlage I, voetnoot 6).

([28]) Bijlage I, hoofdstuk II, punt 2, a). Dit geldt niet wanneer een organisatie persoonsgegevens verstrekt aan een verwerker die namens haar en volgens haar instructies handelt (bijlage I, hoofdstuk II, punt 2, b). In dit geval moet de organisatie echter een contract hebben en ervoor zorgen dat het *Accountability for Onward Transfer Principle* (beginsel van verantwoording voor de verdere doorgifte) wordt nageleefd, zoals nader beschreven in overweging 43. Bovendien kan het keuzebeginsel (evenals het *Notice Principle* — kennisgevingsbeginsel) worden beperkt wanneer persoonsgegevens worden verwerkt in het kader van due diligence-onderzoeken (als onderdeel van een mogelijke fusie of overname) of audits, voor zover en zolang dat nodig is om aan wettelijke vereisten of vereisten van algemeen belang te voldoen, of voor zover en zolang de toepassing van deze beginselen de legitieme belangen van de organisatie in de specifieke context van due diligence-onderzoeken of audits zou schaden (bijlage I, hoofdstuk III, punt 4). Aanvullend beginsel 15 (bijlage I, hoofdstuk III, punt 15, a) en b) voorziet ook in een uitzondering op het keuzebeginsel (alsook op het kennisgevingsbeginsel en het beginsel van verantwoording voor de verdere doorgifte) voor persoonsgegevens uit openbare bronnen (tenzij de EU-gegevensexporteur aangeeft dat de informatie onderworpen is aan beperkingen die de toepassing van die beginselen vereisen) of persoonsgegevens die zijn verzameld uit bestanden die voor iedereen toegankelijk zijn (zolang zij niet worden gecombineerd met niet voor het publiek toegankelijke informatie uit bestanden en alle voorwaarden voor raadpleging worden nageleefd). Evenzo voorziet aanvullend beginsel 14 (bijlage I, hoofdstuk III, punt 14, f)) in een uitzondering op het keuzebeginsel (alsook op het kennisgevingsbeginsel en het beginsel van verantwoording voor de verdere doorgifte) voor de verwerking van persoonsgegevens door een farmaceutisch bedrijf of een bedrijf voor medische hulpmiddelen ten behoeve van de bewaking van de veiligheid en de doeltreffendheid van producten, voor zover de naleving van de beginselen de naleving van wettelijke voorschriften in de weg staat.

([29]) Dit geldt voor alle gegevensdoorgiften in het kader van het EU-VS-DPF, ook wanneer het gaat om gegevens die in het kader van een arbeidsverhouding zijn verzameld. Een gecertificeerde Amerikaanse organisatie mag derhalve in beginsel personeelsgegevens gebruiken voor verschillende, niet aan de arbeidsverhouding gerelateerde doeleinden (bv. bepaalde marketingcommunicatie), maar zij moet het verbod op onverenigbare verwerking eerbiedigen en daarenboven mag zij dit alleen doen met inachtneming van het kennisgevingsbeginsel en het keuzebeginsel. Bij uitzondering mag een organisatie persoonsgegevens gebruiken voor een aanvullend verenigbaar doeleinde zonder het kennisgevings- of het keuzebeginsel toe te passen, maar uitsluitend voor zover en zolang het noodzakelijk is om te voorkomen dat afbreuk wordt gedaan aan de mogelijkheid van die organisatie om besluiten inzake bevorderingen of benoemingen of andere besluiten ten aanzien van de werknemers te nemen (zie bijlage I, hoofdstuk III, punt 9, b), iv)). Het verbod voor de Amerikaanse organisatie om de werknemer die daarvoor kiest, te straffen, onder meer door diens carrièremogelijkheden te beperken, zal ervoor zorgen dat de werknemer ondanks de verhouding van ondergeschiktheid en inherente afhankelijkheid niet onder druk wordt gezet en dus een echte vrije keuze kan maken. Zie bijlage I, hoofdstuk III, punt 9, b), i).

2.2.2 ***Verwerking van bijzondere categorieën van persoonsgegevens***

(16) Wanneer "bijzondere categorieën" gegevens worden verwerkt, moeten bijzondere waarborgen bestaan.

(17) Overeenkomstig het keuzebeginsel gelden specifieke waarborgen voor de verwerking van "gevoelige informatie", d. w.z. persoonsgegevens over medische of gezondheidstoestanden, ras of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen, vakbondslidmaatschap, informatie over het seksleven van de natuurlijke persoon of andere informatie die van derden is ontvangen en door die partij als gevoelig wordt aangemerkt en behandeld ([30]). Dit betekent dat alle gegevens die krachtens de Uniewetgeving inzake gegevensbescherming als gevoelig worden beschouwd (waaronder gegevens over seksuele geaardheid, genetische gegevens en biometrische gegevens) krachtens het EU-VS-DPF door gecertificeerde organisaties als gevoelig zullen worden behandeld.

(18) Als algemene regel geldt dat organisaties de uitdrukkelijke toestemming (d.w.z. opt-in) van natuurlijke personen moeten verkrijgen om gevoelige informatie te gebruiken voor andere doeleinden dan die waarvoor ze oorspronkelijk is verzameld of waarvoor de natuurlijke persoon later toestemming heeft gegeven (via opt-in), of om ze aan derden te verstrekken ([31]).

(19) Die toestemming hoeft niet te worden verkregen in beperkte omstandigheden die vergelijkbaar zijn met soortgelijke uitzonderingen waarin de EU-wetgeving inzake gegevensbescherming voorziet, bijvoorbeeld wanneer de verwerking van gevoelige gegevens in het vitale belang van een persoon is; ze noodzakelijk is om rechtsvorderingen geldend te maken; of noodzakelijk is voor het verstrekken van medische zorg of het stellen van een diagnose ([32]).

2.2.3 ***Nauwkeurigheid, beveiliging en minimale verwerking van gegevens***

(20) De gegevens moeten juist zijn en zo nodig worden geactualiseerd. Ze moeten ook toereikend en ter zake dienend zijn en beperkt blijven tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt en mogen in principe niet langer worden bewaard dan noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

(21) Overeenkomstig het beginsel van gegevensintegriteit en doelbinding ([33]) moeten de persoonsgegevens beperkt blijven tot hetgeen relevant is voor het doel van de verwerking. Bovendien moeten organisaties, voor zover dat nodig is voor de doeleinden van de verwerking, redelijke stappen ondernemen om ervoor te zorgen dat de persoonsgegevens betrouwbaar zijn voor het beoogde gebruik en correct, volledig en actueel zijn.

(22) Bovendien mag persoonlijke informatie slechts worden opgeslagen in een vorm die een natuurlijke persoon identificeert of identificeerbaar maakt (en dus in de vorm van persoonsgegevens) ([34]), zolang dit het doel of de doeleinden dient waarvoor die informatie oorspronkelijk is verzameld of waarvoor de natuurlijke persoon later overeenkomstig het keuzebeginsel toestemming heeft gegeven. Deze verplichting belet niet dat organisaties persoonlijke informatie voor langere perioden blijven verwerken, maar alleen voor de termijn en in de mate dat die verwerking redelijkerwijs een van de volgende specifieke doeleinden dient die vergelijkbaar zijn met soortgelijke uitzonderingen waarin de EU-wetgeving inzake gegevensbescherming voorziet: archivering in het openbaar belang, journalistiek, literatuur en kunst, wetenschappelijk en historisch onderzoek en statistische analyse ([35]). Wanneer persoonsgegevens voor een van deze doeleinden worden bewaard, is de verwerking ervan onderworpen aan de waarborgen van de beginselen ([36]).

(23) Persoonsgegevens moeten ook op een dusdanige manier worden verwerkt dat de beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Daartoe moeten verwerkingsverantwoordelijken en verwerkers passende technische of organisatorische maatregelen treffen om de persoonsgegevens te beschermen tegen mogelijke bedreigingen. Deze maatregelen moeten worden beoordeeld met inachtneming van de stand van de techniek, de daaraan verbonden kosten en de aard, de reikwijdte, de context en de doeleinden van de verwerking, alsmede de risico's voor de rechten van natuurlijke personen.

([30]) Bijlage I, hoofdstuk II, punt 2, c).
([31]) Bijlage I, hoofdstuk II, punt 2, c).
([32]) Bijlage I, hoofdstuk III, punt 1.
([33]) Bijlage I, hoofdstuk II, punt 5.
([34]) Zie bijlage I, voetnoot 7, waarin wordt verduidelijkt dat een natuurlijke persoon als "identificeerbaar" wordt beschouwd zolang een organisatie of een derde partij die persoon redelijkerwijs kan identificeren, rekening houdend met de identificatiemiddelen die redelijkerwijs kunnen worden gebruikt (rekening houdend met onder meer de kosten en de tijd die nodig zijn voor de identificatie en de beschikbare technologie op het tijdstip van de verwerking).
([35]) Bijlage I, hoofdstuk II, punt 5, b).
([36]) *Zie vorige voetnoot*.

(24) In het kader van het EU-VS-DPF wordt dit gewaarborgd door het *Security Principle* (beveiligingsbeginsel), dat, naar analogie van artikel 32 van Verordening (EU) 2016/679, voorschrijft dat redelijke en passende beveiligingsmaatregelen moeten worden genomen, rekening houdend met de risico's van de verwerking en de aard van de gegevens ([37]).

2.2.4 ***Transparantie***

(25) Betrokkenen moeten worden ingelicht over de belangrijkste kenmerken van de verwerking van hun persoonsgegevens.

(26) Dit wordt gewaarborgd door het *Notice Principle* (kennisgevingsbeginsel) ([38]), dat, analoog aan de transparantievereisten van Verordening (EU) 2016/679, organisaties verplicht om betrokkenen te informeren over onder meer i) de deelname van de organisatie aan het DPF, ii) de aard van de verzamelde gegevens, iii) het doel van de verwerking, iv) het type of de identiteit van derden waaraan persoonsgegevens kunnen worden verstrekt en de doeleinden daarvoor, v) hun individuele rechten, vi) hoe zij contact kunnen opnemen met de organisatie en vii) de beschikbare verhaalmechanismemogelijkheden.

(27) Deze kennisgeving moet in duidelijke en opvallende taal worden gedaan wanneer natuurlijke personen voor het eerst om persoonsgegevens wordt gevraagd of zo spoedig mogelijk daarna, maar in ieder geval voordat de gegevens worden gebruikt voor een wezenlijk ander (maar verenigbaar) doel dan het doel waarvoor ze zijn verzameld, of voordat ze aan derden worden verstrekt ([39]).

(28) Bovendien moeten organisaties hun privacybeleid dat de beginselen weerspiegelt, openbaar maken (of, in het geval van personeelsgegevens, gemakkelijk toegankelijk maken voor de betrokken personen) en links verstrekken naar de website van het ministerie van Handel (met nadere informatie over certificering, de rechten van de betrokkenen en de beschikbare beroepsmogelijkheden), de lijst van deelnemende organisaties aan het kader voor gegevensbescherming (DPF-lijst) en de website van een passende aanbieder van alternatieve geschillenbeslechting ([40]).

2.2.5 ***Individuele rechten***

(29) Betrokkenen moeten bepaalde rechten hebben die kunnen worden afgedwongen ten opzichte van de verwerkingsverantwoordelijke of de verwerker, en met name het recht op inzage van de gegevens, het recht om bezwaar te maken tegen de verwerking en het recht op rectificatie of wissing van de gegevens.

(30) Het *Access Principle* (toegangsbeginsel) ([41]) van het EU-VS-DPF verleent natuurlijke personen dergelijke rechten. In het bijzonder hebben betrokkenen het recht om, zonder opgave van redenen, van een organisatie te verlangen dat deze bevestigt of zij persoonsgegevens over hen verwerkt; de gegevens aan hen te laten meedelen; en informatie te verkrijgen over het doel van de verwerking, de categorieën persoonsgegevens die worden verwerkt en de (categorieën) ontvangers aan wie de gegevens worden verstrekt ([42]). Organisaties moeten binnen een redelijke termijn reageren op verzoeken om toegang ([43]). Een organisatie kan redelijke grenzen stellen aan het aantal keren

([37]) Bijlage I, hoofdstuk II, punt 4, a). Wat personeelsgegevens betreft, verplicht het EU-VS-DPF werkgevers bovendien tegemoet te komen aan de privacyvoorkeuren van werknemers door de toegang tot de persoonsgegevens te beperken, bepaalde gegevens anoniem te maken of codes of pseudoniemen toe te kennen (bijlage I, hoofdstuk III, punt 9, b), iii).

([38]) Bijlage I, hoofdstuk II, punt 1.

([39]) Bijlage I, hoofdstuk II, punt 1, b). Aanvullend beginsel 14 (bijlage I, hoofdstuk III, punt 14, b) en c) bevat specifieke bepalingen voor de verwerking van persoonsgegevens in het kader van gezondheidsonderzoek en klinische proeven. Dit beginsel staat met name organisaties toe gegevens van klinische proeven te verwerken, zelfs nadat een persoon zich uit de proef heeft teruggetrokken, als dit duidelijk is vermeld in de kennisgeving die is verstrekt toen de persoon instemde met zijn of haar deelname. Ook wanneer een EU-VS-DPF-organisatie persoonsgegevens ontvangt voor gezondheidsonderzoek, mag zij deze alleen voor een nieuwe onderzoeksactiviteit gebruiken overeenkomstig het kennisgevingsbeginsel en het keuzebeginsel. In dat geval moet de kennisgeving aan de natuurlijke persoon in beginsel informatie bevatten over een toekomstig specifiek gebruik van de gegevens (bijvoorbeeld verwante studies). Wanneer het niet mogelijk is om van meet af aan alle toekomstige toepassingen van de gegevens op te nemen (omdat een nieuw onderzoekgebruik zou kunnen voortvloeien uit nieuwe inzichten of medische/onderzoeksontwikkelingen), moet een verklaring worden opgenomen dat de gegevens in toekomstige niet-verwachte medische en farmaceutische onderzoeksactiviteiten kunnen worden gebruikt. Indien dergelijk verder gebruik niet strookt met de algemene onderzoeksdoeleinden waarvoor de gegevens zijn verzameld (d.w.z. als de nieuwe doeleinden wezenlijk verschillen van, maar nog altijd verenigbaar zijn met het oorspronkelijke doeleinde, zie overwegingen 14 en 15), moet opnieuw toestemming (d.w.z. opt-in) worden verkregen. Zie voorts de specifieke beperkingen/uitzonderingen op het kennisgevingsbeginsel die in voetnoot 28 worden beschreven.

([40]) Bijlage I, hoofdstuk III, punt 6, d).

([41]) Zie ook het aanvullende beginsel inzake toegang (bijlage I, hoofdstuk III, 8)).

([42]) Bijlage I, hoofdstuk III, punt 8, a), i) en ii).

([43]) Bijlage I, hoofdstuk III, punt 8, i).

dat binnen een bepaalde periode aan verzoeken om toegang van een bepaalde persoon wordt voldaan en kan een vergoeding vragen die niet buitensporig is, bijvoorbeeld wanneer verzoeken duidelijk buitensporig zijn, met name vanwege hun repetitieve karakter ([44]).

(31) Het recht van toegang kan alleen worden beperkt in uitzonderlijke omstandigheden die vergelijkbaar zijn met die waarin de EU-wetgeving inzake gegevensbescherming voorziet, met name wanneer de legitieme rechten van anderen zouden worden geschonden; wanneer de lasten of kosten van het verlenen van toegang niet in verhouding zouden staan tot de risico's voor de persoonlijke levenssfeer van de natuurlijke persoon in de omstandigheden van het geval (hoewel lasten en kosten geen doorslaggevende factoren zijn om te bepalen of het verlenen van toegang redelijk is); voor zover openbaarmaking in strijd zou zijn met belangrijke openbare belangen, zoals de nationale of openbare veiligheid, of defensie; wanneer de informatie vertrouwelijke commerciële informatie bevat; of wanneer de informatie uitsluitend voor onderzoeks- of statistische doeleinden wordt verwerkt ([45]). Het weigeren of het beperken van een recht moet nodig en naar behoren gerechtvaardigd zijn, waarbij de organisatie moet aantonen dat aan deze voorschriften is voldaan ([46]). Wanneer de organisatie die beoordeling verricht, moet zij in het bijzonder rekening houden met de belangen van de natuurlijke persoon ([47]). Wanneer het mogelijk is informatie te scheiden van andere gegevens waarvoor een beperking geldt, moet de organisatie de vertrouwelijke informatie bewerken en de niet-vertrouwelijke informatie beschikbaar stellen ([48]).

(32) Bovendien hebben betrokkenen het recht onjuiste gegevens te laten corrigeren of wijzigen en gegevens die in strijd met de beginselen ([49]) zijn verwerkt, te laten wissen. Tevens hebben natuurlijke personen, zoals uiteengezet in overweging 15, het recht bezwaar te maken tegen/zich te verzetten tegen de verwerking van hun gegevens voor wezenlijk andere (maar verenigbare) doeleinden dan die waarvoor de gegevens zijn verzameld en tegen de verstrekking van hun gegevens aan derden. Wanneer persoonsgegevens worden gebruikt voor direct marketing, hebben personen een algemeen recht om zich te allen tijde te verzetten tegen de verwerking ([50]).

(33) De beginselen hebben niet specifiek betrekking op besluiten die gevolgen hebben voor de betrokkene en die uitsluitend gebaseerd zijn op de geautomatiseerde verwerking van persoonsgegevens. Wat betreft de persoonsgegevens die in de Europese Unie zijn verzameld, wordt elk besluit dat is gebaseerd op geautomatiseerde verwerking, echter doorgaans genomen door de verwerkingsverantwoordelijke in de Unie (die een directe relatie met de betrokkene heeft) en is daarom onderworpen aan Verordening (EU) 2016/679 ([51]). Dit omvat doorgiftescenario's waarin de verwerking wordt uitgevoerd door een buitenlandse (bijvoorbeeld Amerikaanse) bedrijfsexploitant die handelt als verwerker namens de verwerkingsverantwoordelijke in de Unie (of als subverwerker die handelt namens de verwerker in de Unie, die de gegevens heeft ontvangen van een EU-verwerkingsverantwoordelijke die ze heeft verzameld) die op deze basis de beslissing neemt.

(34) Dit werd bevestigd door een studie waartoe de Commissie in 2018 opdracht had gegeven in het kader van de tweede jaarlijkse evaluatie van de werking van het privacyschild ([52]), waarin werd geconcludeerd dat er op dat moment geen aanwijzingen waren dat er normaliter geautomatiseerde besluitvorming werd uitgevoerd door privacyschildorganisaties op basis van persoonsgegevens die in het kader van het privacyschild waren doorgegeven.

([44]) Bijlage I, hoofdstuk III, punt 8, f), i) en ii), en punt 8, g).
([45]) Bijlage I, hoofdstuk III, punt 4; punt 8, b), c), e); punt 14, e), f) en punt 15, d).
([46]) Bijlage I, hoofdstuk III, punt 8, e), ii). De organisatie moet de natuurlijke persoon in kennis stellen van de redenen voor de weigering/beperking en een contactpunt opgeven voor verdere vragen, hoofdstuk III, punt 8, a), iii).
([47]) Bijlage I. hoofdstuk III, punt 8, a), ii) en iii).
([48]) Bijlage I, hoofdstuk III, punt 8, a), i).
([49]) Bijlage I, hoofdstuk II, punt 6 en hoofdstuk III, punt 8, a), i).
([50]) Bijlage I, hoofdstuk III, punt 8, 12).
([51]) In het uitzonderlijke geval waarin de Amerikaanse bedrijfsexploitant een directe relatie met de betrokkene in de Unie heeft, komt dit daarentegen doorgaans doordat hij of zij zich direct tot de betrokkene in de Unie heeft gericht door goederen of diensten aan te bieden of zijn of haar gedrag te volgen. In dit scenario valt de Amerikaanse exploitant zelf binnen de werkingssfeer van Verordening (EU) 2016/679 (artikel 3, lid 2) en moet hij of zij dus rechtstreeks voldoen aan de gegevensbeschermingswetgeving van de Unie.
([52]) SWD(2018) 497 final, punt 4.1.5. De studie was gericht op i) de mate waarin privacyschildorganisaties in de VS besluiten nemen die gevolgen hebben voor natuurlijke personen op basis van de geautomatiseerde verwerking van persoonsgegevens die in het kader van het privacyschild door bedrijven in de EU zijn doorgegeven; en ii) de waarborgen voor natuurlijke personen die het Amerikaanse federale recht biedt voor dit soort situaties en de voorwaarden waaronder deze waarborgen van toepassing zijn.

(35) In ieder geval biedt de Amerikaanse wetgeving op gebieden waar ondernemingen waarschijnlijk een beroep doen op de geautomatiseerde verwerking van persoonsgegevens om beslissingen te nemen die de natuurlijke persoon betreffen (bv. kredietverschaffing, aanbiedingen van hypothecaire leningen, werkgelegenheid, huisvesting en verzekeringen), specifieke bescherming tegen ongunstige beslissingen ([53]). Die wetten voorzien er doorgaans in dat natuurlijke personen het recht hebben om te worden geïnformeerd over de specifieke redenen die aan de beslissing (bv. de weigering van een krediet) ten grondslag liggen, om onvolledige of niet correcte informatie te betwisten (alsook het feit dat met onrechtmatige factoren rekening is gehouden), en om verhaal te halen. Op het gebied van consumentenkrediet bevatten de Fair Credit Reporting Act (wet billijke kredietrapportage, hierna "FCRA") en de Equal Credit Opportunity Act (wet gelijke kredietkansen, hierna "ECOA") waarborgen die de consument een vorm van recht op uitleg bieden evenals een recht om de beslissing aan te vechten. Deze wetten zijn relevant op een groot aantal gebieden, waaronder krediet, werkgelegenheid, huisvesting en verzekeringen. Bovendien bieden bepaalde antidiscriminatiewetten, zoals Titel VII van de Civil Rights Act (wet burgerrechten) en de Fair Housing Act (wet billijke huisvesting), natuurlijke personen bescherming tegen modellen die worden gebruikt bij geautomatiseerde besluitvorming die kunnen leiden tot discriminatie op grond van bepaalde kenmerken, en verlenen zij personen het recht om dergelijke, ook geautomatiseerde, besluiten aan te vechten. Met betrekking tot gezondheidsinformatie creëert de privacyregel van de Health Insurance Portability and Accountability Act (wet overdraagbaarheid en verantwoordingsplicht gezondheidsverzekering, hierna "HIPAA") bepaalde rechten die vergelijkbaar zijn met die van Verordening (EU) 2016/679 wat betreft de toegang tot persoonlijke gezondheidsinformatie. Bovendien moeten medische zorgverleners op grond van richtsnoeren van de Amerikaanse autoriteiten informatie ontvangen waarmee zij personen op de hoogte kunnen stellen van geautomatiseerde besluitvormingssystemen die in de medische sector worden gebruikt ([54]).

(36) Deze regels bieden dan ook soortgelijke bescherming als die waarin de EU-wetgeving inzake gegevensbescherming voorziet in de onwaarschijnlijke situatie waarin de EU-VS-DPF-organisatie zelf geautomatiseerde besluiten zou nemen.

2.2.6 ***Beperkingen op verdere doorgifte***

(37) Het beschermingsniveau dat wordt geboden voor persoonsgegevens die worden doorgegeven vanuit de Unie naar organisaties in de Verenigde Staten mag niet worden ondermijnd door de verdere doorgifte van dergelijke gegevens aan ontvangers in de Verenigde Staten of in een ander derde land.

(38) Volgens het *Accountibility for Onward Transfer Principle* (beginsel van verantwoording voor de verdere doorgifte) ([55]) gelden er bijzondere regels voor zogenaamde "verdere doorgiften", d.w.z. doorgiften van persoonsgegevens van een EU-VS-DPF-organisatie naar een derde-verwerkingsverantwoordelijke of -verwerker, ongeacht of die laatste in de Verenigde Staten of een derde land buiten de Verenigde Staten (en de Unie) is gevestigd. Verdere doorgifte kan alleen plaatsvinden i) voor beperkte en gespecificeerde doeleinden, ii) op basis van een overeenkomst tussen de EU-VS-DPF-organisatie en de derde ([56]) (of een vergelijkbare regeling binnen een concern ([57])) en iv) alleen als die overeenkomst de derde verplicht hetzelfde beschermingsniveau te bieden als het niveau dat door de beginselen wordt gewaarborgd.

(39) Deze verplichting om hetzelfde beschermingsniveau te bieden als door de beginselen wordt gewaarborgd, in combinatie met het beginsel van gegevensintegriteit en doelbinding, houdt met name in dat de derde de aan hem doorgegeven persoonsgegevens alleen mag verwerken voor doeleinden die niet onverenigbaar zijn met de doeleinden waarvoor ze zijn verzameld of waarvoor de betrokkene later toestemming heeft gegeven (overeenkomstig het keuzebeginsel).

([53]) Zie bv. de Equal Credit Opportunity Act (15 U.S.C. § 1691 e.v.), de Fair Credit Reporting Act (15 U.S.C. § 1681 e.v.) of de Fair Housing Act (42 U.S.C. § 3601 e.v.). Bovendien hebben de Verenigde Staten de beginselen inzake artificiële intelligentie van de Organisatie voor Economische Samenwerking en Ontwikkeling onderschreven, die onder meer beginselen inzake transparantie, verklaarbaarheid, veiligheid en verantwoording omvatten.

([54]) Zie bijvoorbeeld de richtsnoeren op 2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? [2042 — Tot welke persoonlijke gezondheidsinformatie van hun zorgverleners en gezondheidsplannen hebben personen krachtens de HIPAA recht op toegang?] | HHS.gov

([55]) Zie bijlage I, hoofdstuk II, punt 3, en het aanvullende beginsel inzake verplichte overeenkomsten voor de verdere doorgifte (bijlage I, hoofdstuk III, punt 10).

([56]) Als uitzondering op dit algemene beginsel kan een organisatie persoonsgegevens van een klein aantal werknemers doorgeven zonder een overeenkomst met de ontvanger te sluiten voor incidentele werkgerelateerde operationele behoeften, bijvoorbeeld het boeken van een vlucht, hotelkamer of verzekeringsdekking. Ook in dit geval moet de organisatie echter nog steeds voldoen aan het kennisgevings-beginsel en het keuzebeginsel (zie bijlage I, hoofdstuk III, punt 9, e)).

([57]) Zie het aanvullend beginsel inzake verplichte overeenkomsten voor de verdere doorgifte (bijlage I, hoofdstuk III, punt 10, b)). Dit beginsel maakt ook doorgiften op basis van niet-contractuele instrumenten (bv. nalevings- en controleprogramma's binnen een groep) mogelijk, maar de tekst maakt duidelijk dat die instrumenten altijd "de continuïteit van de bescherming van persoonlijke informatie in het kader van de beginselen moeten garanderen". Omdat de gecertificeerde Amerikaanse organisatie verantwoordelijk zal blijven voor de naleving van de beginselen, is er voor haar daarenboven een sterke stimulans om instrumenten te gebruiken die inderdaad doeltreffend zijn in de praktijk.

(40) Het beginsel van verantwoording voor de verdere doorgifte moet worden gelezen in samenhang met het kennisgevingsbeginsel en, in het geval van een verdere doorgifte naar een derde-verwerker ([58]), het keuzebeginsel, volgens welke betrokkenen moeten worden geïnformeerd (onder andere) over de aard/identiteit van derde-ontvangers, het doel van de verdere doorgifte en de geboden keuze en zich kunnen verzetten (opt-out) of, in het geval van gevoelige gegevens "uitdrukkelijke bevestigende toestemming" moeten geven (opt-in) voor de verdere doorgiften.

(41) De verplichting hetzelfde beschermingsniveau te bieden als het door de beginselen vereiste niveau geldt voor alle derden die bij de verwerking van de op die manier doorgegeven gegevens zijn betrokken (in de Verenigde Staten of een ander derde land), alsook wanneer de oorspronkelijke derde-ontvanger zelf die gegevens naar een andere derde-ontvanger doorgeeft, bijvoorbeeld met het oog op subverwerking.

(42) In alle gevallen moet de overeenkomst met de derde-ontvanger erin voorzien dat die laatste de EU-VS-DPF-organisatie ervan in kennis zal stellen als hij vaststelt dat hij niet langer aan die verplichting kan voldoen. Wanneer een dergelijke vaststelling wordt gedaan, moet de verwerking door de derde worden stopgezet of moeten andere redelijke en passende stappen worden ondernomen om de situatie te verhelpen ([59]).

(43) In het geval van een verdere doorgifte naar een derde-vertegenwoordiger (m.a.w. een verwerker) geldt aanvullende bescherming. In een dergelijk geval moet de Amerikaanse organisatie ervoor zorgen dat de vertegenwoordiger alleen in haar opdracht handelt en redelijke en passende stappen ondernemen i) om ervoor te zorgen dat de vertegenwoordiger daadwerkelijk de doorgegeven persoonlijke informatie verwerkt op een manier die in overeenstemming is met de verplichtingen van de organisatie uit hoofde van de beginselen, en ii) om na kennisgeving de niet-toegestane verwerking stop te zetten en te verhelpen ([60]). De organisatie kan door het ministerie van Handel worden verplicht om een samenvatting of een representatief exemplaar van de privacybepalingen van het contract te verstrekken ([61]). Wanneer zich in een (sub)verwerkingsketen nalevingsproblemen voordoen, wordt de organisatie die optreedt als verantwoordelijke voor de verwerking van de persoonsgegevens in beginsel aansprakelijk gesteld, zoals bepaald in het *Recourse, Enforcement and Liability Principle* (beginsel inzake verhaal, handhaving en aansprakelijkheid), behalve wanneer zij bewijst dat zij niet verantwoordelijk is voor de gebeurtenis die aanleiding heeft gegeven tot de schade ([62]).

2.2.7 ***Verantwoording***

(44) Volgens het verantwoordingsbeginsel moeten entiteiten die gegevens verwerken passende technische en organisatorische maatregelen nemen om doeltreffend hun verplichtingen inzake gegevensbescherming te kunnen naleven, en moeten zij de naleving daarvan kunnen aantonen, in het bijzonder ten overstaan van de bevoegde toezichthoudende autoriteit.

(45) Zodra een organisatie vrijwillig heeft gekozen voor certificering ([63]) in het kader van het EU-VS-DPF, is haar daadwerkelijke naleving van de beginselen verplicht en afdwingbaar. Krachtens het beginsel inzake verhaal, handhaving en aansprakelijkheid ([64]) moeten de EU-VS-DPF-organisaties voorzien in doeltreffende mechanismen om de naleving van de beginselen te waarborgen. Organisaties moeten ook maatregelen nemen om te controleren ([65]) of hun privacybeleid in overeenstemming is met de beginselen en daadwerkelijk wordt nageleefd. Dit kan gebeuren door middel van hetzij een systeem van zelfbeoordeling, dat interne procedures moet omvatten om te garanderen dat de werknemers worden opgeleid om het privacybeleid van de organisatie uit te voeren en dat de naleving periodiek op objectieve wijze wordt geëvalueerd, hetzij externe evaluaties van de naleving, waarvan de methoden onder meer kunnen bestaan in audits, steekproefsgewijze controles of het gebruik van technologische hulpmiddelen.

([58]) Natuurlijke personen zullen geen opt-outrecht hebben wanneer de persoonsgegevens worden doorgegeven naar een derde die optreedt als vertegenwoordiger van een Amerikaanse organisatie om namens haar en volgens haar instructies taken uit te voeren. Dit vereist echter een overeenkomst met de vertegenwoordiger en de Amerikaanse organisatie zal verantwoordelijk zijn voor het garanderen van de bescherming in het kader van de beginselen door het uitoefenen van haar bevoegdheid tot het geven van instructies.

([59]) De situatie is verschillend naargelang de derde een verwerkingsverantwoordelijke of een verwerker (vertegenwoordiger) is. In het eerste scenario moet de overeenkomst met de derde erin voorzien dat hij de verwerking stopzet of andere redelijke en passende stappen onderneemt om de situatie te verhelpen. In het tweede scenario moet de EU-VS-DPF-organisatie — als de verantwoordelijke voor de verwerking door de vertegenwoordiger volgens de gegeven instructies — die stappen ondernemen. Zie bijlage I, hoofdstuk II, punt 3.

([60]) Bijlage I, hoofdstuk II, punt 3, b).

([61]) *Zie vorige voetnoot.*

([62]) Bijlage I, hoofdstuk II, punt 7, d).

([63]) Zie ook het aanvullend beginsel inzake zelfcertificering (bijlage I, hoofdstuk III, punt 6).

([64]) Zie ook het aanvullend beginsel inzake geschillenbeslechting en handhaving (bijlage I, hoofdstuk III, punt 11).

([65]) Zie ook het aanvullend beginsel inzake controle (bijlage I, hoofdstuk III, punt 7).

(46) Bovendien moeten organisaties gegevens over de uitvoering van hun EU-VS-DPF-praktijken bewaren en op verzoek beschikbaar stellen in het kader van een onderzoek of een klacht over niet-naleving aan een onafhankelijke instantie voor geschillenbeslechting of een bevoegde handhavingsautoriteit ([66]).

2.3 **Beheer, toezicht en handhaving**

(47) Het EU-VS-DPF wordt beheerd en gecontroleerd door het ministerie van Handel. Het kader voorziet in toezichts- en handhavingsmechanismen om na te gaan en te garanderen dat EU-VS-DPF-organisaties de beginselen naleven en dat tegen niet-naleving wordt opgetreden. Die mechanismen zijn beschreven in de beginselen (bijlage I) en de verbintenissen van het ministerie van Handel (bijlage III), de FTC (bijlage IV) en het ministerie van Vervoer (bijlage V).

2.3.1 ***(Her)certificering***

(48) Om zich in het kader van het EU-VS-DPF te certificeren (of jaarlijks te hercertificeren) moeten organisaties publiekelijk verklaren dat zij zich ertoe verbinden de beginselen na te leven, hun privacybeleid beschikbaar stellen en dit volledig uitvoeren ([67]). Als onderdeel van hun (her)certificeringsaanvraag moeten organisaties het ministerie van Handel informatie verstrekken over onder meer de naam van de betrokken organisatie, een beschrijving van de doeleinden waarvoor de organisatie persoonsgegevens zal verwerken, de persoonsgegevens die onder de certificering vallen, alsmede de gekozen verificatiemethode, het relevante onafhankelijke verhaalmechanisme en de wettelijke instantie die bevoegd is om de naleving van de beginselen te handhaven ([68]).

(49) Organisaties kunnen persoonsgegevens ontvangen op grond van het EU-VS-DPF vanaf de datum waarop zij door het ministerie van Handel op de DPF-lijst zijn geplaatst. Om rechtszekerheid te garanderen en "valse beweringen" te voorkomen, mogen organisaties die voor het eerst gecertificeerd worden, niet publiekelijk verwijzen naar hun naleving van de beginselen voordat het ministerie van Handel heeft vastgesteld dat de certificering van de organisatie volledig is en de organisatie is toegevoegd aan de DPF-lijst ([69]). Om voor het ontvangen van persoonsgegevens uit de Unie gebruik te mogen blijven maken van het EU-VS-DPF, moeten dergelijke organisaties hun deelname aan het kader jaarlijks opnieuw certificeren. Wanneer een organisatie om welke reden dan ook het EU-VS-DPF verlaat, moet zij alle openbare verklaringen verwijderen waarmee wordt gesuggereerd dat de organisatie blijft deelnemen aan het kader ([70]).

(50) Zoals blijkt uit de verbintenissen in bijlage III, zal het ministerie van Handel nagaan of organisaties aan alle certificeringseisen voldoen en een (openbaar) privacybeleid hebben ingevoerd dat de krachtens het kennisgevingsbeginsel vereiste informatie bevat ([71]). Voortbouwend op de ervaring met het (her)certificeringsproces in het kader van het privacyschild zal het ministerie van Handel een aantal controles uitvoeren, onder meer om na te gaan of het privacybeleid van organisaties een hyperlink bevat naar het juiste klachtenformulier op de website van het relevante mechanisme voor geschillenbeslechting en, wanneer verschillende entiteiten en dochterondernemingen van één organisatie bij een certificeringsaanvraag zijn betrokken, of het privacybeleid van elk van die entiteiten aan de certificeringsvereisten voldoet en gemakkelijk beschikbaar is voor betrokkenen ([72]). Bovendien zal het ministerie van Handel, waar nodig, kruiscontroles uitvoeren met de FTC en het ministerie van Vervoer om na te gaan of de organisaties onderworpen zijn aan de toezichthoudende instantie die zij in hun (her)certificeringsaanvragen hebben vermeld, en zal het samenwerken met instanties voor alternatieve geschillenbeslechting om na te gaan of de organisaties geregistreerd zijn voor het onafhankelijke verhaalmechanisme dat zij in hun (her)certificeringsaanvraag hebben vermeld ([73]).

([66]) Bijlage I, hoofdstuk III, punt 7.
([67]) Bijlage I, hoofdstuk I, punt 2.
([68]) Bijlage I, hoofdstuk III, punt 6, b), en bijlage III, hoofdstuk "De inachtneming van de vereisten inzake zelfcertificering controleren".
([69]) Bijlage I, voetnoot 12.
([70]) Bijlage I, hoofdstuk III, punt 6, h).
([71]) Bijlage I, hoofdstuk III, punt 6, a), en voetnoot 12, alsook bijlage III, hoofdstuk "De inachtneming van de vereisten inzake zelfcertificering controleren".
([72]) Bijlage III, hoofdstuk "De inachtneming van de vereisten inzake zelfcertificering controleren".
([73]) Evenzo zal het ministerie van Handel samenwerken met de derde partij die zal dienen als bewaarder van de financiële middelen die via de panelvergoeding voor gegevensbeschermingsautoriteiten (zie overweging 73) worden geïnd, om na te gaan of organisaties die de gegevensbeschermingsautoriteiten als hun onafhankelijk verhaalmechanisme kiezen, de vergoeding voor het betrokken jaar hebben betaald. Zie bijlage III, hoofdstuk "De inachtneming van de vereisten inzake zelfcertificering controleren".

(51) Het ministerie van Handel zal de organisaties meedelen dat zij, om de (her)certificering te voltooien, alle tijdens de evaluatie geconstateerde problemen moeten aanpakken. Indien een organisatie niet reageert binnen een door het ministerie van Handel vastgestelde termijn (voor hercertificering wordt bijvoorbeeld verwacht dat het proces binnen 45 dagen wordt afgerond) ([74]) of anderszins haar certificering niet voltooit, wordt de indiening als stopgezet beschouwd. In dat geval kan elke onjuiste voorstelling van zaken over deelname aan of naleving van het EU-VS-DPF aanleiding geven tot handhavingsmaatregelen van de FTC of het ministerie van Vervoer ([75]).

(52) Voor een correcte toepassing van het EU-VS-DPF moeten de belanghebbenden, zoals de betrokkenen, degenen die gegevens naar het buitenland doorgeven en de nationale gegevensbeschermingsautoriteiten kunnen vaststellen welke organisaties de beginselen onderschrijven. Om deze transparantie bij het "ingangspunt" te waarborgen, heeft het ministerie van Handel toegezegd de lijst bij te houden en voor het publiek toegankelijk te maken van de organisaties die door certificering de beginselen hebben onderschreven en die onder de rechtsbevoegdheid vallen van ten minste een van de in de bijlagen IV en V bij dit besluit genoemde handhavingsautoriteiten ([76]). Het ministerie van Handel werkt de lijst bij op basis van de jaarlijks doorgegeven hercertificering van de organisatie en wanneer een organisatie zich terugtrekt of wordt verwijderd uit het EU-VS-DPF. Voorts zal het ministerie van Handel, om ook op het "exitpunt" transparantie te garanderen, een bestand bijhouden en openbaar maken waarin organisaties zijn opgenomen die van de lijst zijn verwijderd, waarbij telkens de reden voor die verwijdering wordt aangegeven ([77]). Ten slotte zal het een link geven naar de webpagina van de FTC over het EU-VS-DPF, waarop de handhavingsacties van de FTC binnen het kader zijn vermeld ([78]).

2.3.2 *Toezicht op de naleving*

(53) Het ministerie van Handel zal via verschillende mechanismen voortdurend toezicht houden op de daadwerkelijke naleving van de beginselen door de EU-VS-DPF-organisaties ([79]). Het zal met name "steekproefsgewijze controles" uitvoeren bij willekeurig geselecteerde organisaties, alsook ad-hocsteekproeven bij specifieke organisaties wanneer potentiële nalevingsproblemen worden vastgesteld (bv. gemeld aan het ministerie van Handel door derden) om na te gaan of i) de contactpunten voor de behandeling van klachten en verzoeken van betrokkenen beschikbaar zijn en reageren; ii) het privacybeleid van de organisatie gemakkelijk beschikbaar is, zowel op haar website als via een hyperlink op de website van het ministerie van Handel; iii) het privacybeleid van de organisatie blijft voldoen aan de certificeringseisen en iv) het door de organisaties gekozen onafhankelijke mechanisme voor geschillenbeslechting beschikbaar is voor de behandeling van klachten ([80]).

(54) Indien er geloofwaardige aanwijzingen zijn dat een organisatie haar verbintenissen in het kader van het EU-VS-DPF niet nakomt (ook indien het ministerie van Handel klachten ontvangt of de organisatie niet bevredigend reageert op vragen van het ministerie van Handel), zal het ministerie van Handel van de organisatie verlangen dat zij een gedetailleerde vragenlijst invult en indient ([81]). Een organisatie die de vragenlijst niet bevredigend en tijdig beantwoordt, wordt doorverwezen naar de bevoegde autoriteit (de FTC of het ministerie van Vervoer) voor eventuele handhavingsmaatregelen ([82]). Als onderdeel van het toezicht op de naleving in het kader van het privacyschild voerde het ministerie van Handel regelmatig de in overweging 53 genoemde steekproefsgewijze

([74]) Bijlage III, voetnoot 2.
([75]) Zie bijlage III, hoofdstuk "De inachtneming van de vereisten inzake zelfcertificering controleren".
([76]) Informatie over het beheer van de DPF-lijst staat in bijlage III (zie de inleiding onder "Beheer en toezicht inzake het kaderprogramma voor gegevensbescherming door het ministerie van Handel") en in bijlage I (hoofdstuk I, punt 3, hoofdstuk I, punt 4, hoofdstuk III, punt 6, d), en hoofdstuk III, punt 11, g)).
([77]) Bijlage III, zie de inleiding onder "Beheer en toezicht inzake het kaderprogramma voor gegevensbescherming door het ministerie van Handel".
([78]) Zie bijlage III, hoofdstuk "De website van het kader voor gegevensbescherming aanpassen aan specifieke doelgroepen".
([79]) Zie bijlage III, hoofdstuk "Periodiek ambtshalve nalevingscontroles en evaluaties van het kaderprogramma voor gegevensbescherming uitvoeren".
([80]) Als onderdeel van zijn toezicht kan het ministerie van Handel verschillende instrumenten gebruiken, waaronder het controleren op gebroken links naar het privacybeleid of het actief volgen van het nieuws voor berichten die geloofwaardig bewijs van niet-naleving leveren.
([81]) Zie bijlage III, hoofdstuk "Periodiek ambtshalve nalevingscontroles en evaluaties van het kaderprogramma voor gegevensbescherming uitvoeren".
([82]) Zie bijlage III, hoofdstuk "Periodiek ambtshalve nalevingscontroles en evaluaties van het kaderprogramma voor gegevensbescherming uitvoeren".

controles uit en hield het voortdurend toezicht op openbare verslagen, waardoor het nalevingsproblemen kon opsporen, aanpakken en oplossen ([83]). Een organisatie wordt in geval van permanente niet-naleving van de beginselen uit de DPF-lijst verwijderd en moet de in het kader van het EU-VS-DPF ontvangen persoonsgegevens terugbezorgen of wissen ([84]).

(55) In andere gevallen van verwijdering, zoals vrijwillige terugtrekking van deelname of verzuim de naleving opnieuw te certificeren, moet de organisatie de gegevens wissen of teruggeven, of mag zij deze bewaren, mits zij jaarlijks aan het ministerie van Handel bevestigt dat zij zich tot de naleving van de beginselen blijft verbinden of met andere toegestane middelen een passende bescherming voor de persoonsgegevens biedt (bv. met behulp van een overeenkomst die de vereisten van de bepalingen dienaangaande van de door de Commissie goedgekeurde modelovereenkomst volledig weerspiegelt) ([85]). In dit geval moet een organisatie een contactpunt binnen de organisatie aanwijzen voor alle vragen in verband met het EU-VS-DPF.

2.3.3 *Valse beweringen van deelname identificeren en aanpakken*

(56) Het ministerie van Handel zal zowel ambtshalve als op basis van klachten (bv. ontvangen van gegevensbeschermingsautoriteiten) eventuele valse beweringen inzake deelname aan het EU-VS-DPF of het onterechte gebruik van het keurmerk van het EU-VS-DPF controleren ([86]). Het ministerie van Handel zal met name voortdurend nagaan of organisaties die i) hun deelname aan het EU-VS-DPF beëindigen, ii) de jaarlijkse hercertificering niet voltooien (d.w.z. ofwel zijn begonnen, maar het jaarlijkse hercertificeringsproces niet tijdig hebben voltooid, ofwel niet eens zijn begonnen met het jaarlijkse hercertificeringsproces), iii) worden geschrapt als deelnemer, met name wegens "permanente niet-naleving", of iv) een initiële certificering niet voltooien (d.w.z. zijn begonnen, maar het initiële certificeringsproces niet tijdig hebben voltooid), verwijzingen naar het EU-VS-DPF die impliceren dat de organisatie actief deelneemt aan het DPF-kader, uit alle relevante gepubliceerde verwijzingen naar het privacybeleid verwijderen ([87]). Het ministerie van Handel zal ook op internet zoeken naar verwijzingen naar het EU-VS-DPF in het privacybeleid van organisaties, onder meer om valse beweringen op te sporen van organisaties die nooit hebben deelgenomen aan het EU-VS-DPF ([88]).

(57) Wanneer het ministerie van Handel constateert dat verwijzingen naar het EU-VS-DPF niet zijn verwijderd of onterecht worden gebruikt, zal het de organisatie informeren over een mogelijke verwijzing naar de FTC/ministerie van Vervoer ([89]). Als een organisatie niet op bevredigende wijze reageert, zal het ministerie van Handel de zaak doorverwijzen naar de bevoegde instantie voor mogelijke handhavingsmaatregelen ([90]). Tegen een verkeerde voorstelling aan het grote publiek over de onderschrijving van de beginselen door een organisatie in de vorm van misleidende verklaringen of praktijken kan handhavend worden opgetreden door de FTC, het ministerie van Vervoer of andere bevoegde Amerikaanse handhavingsautoriteiten. Tegen verkeerde voorstellingen tegenover het ministerie van Handel kan handhavend worden opgetreden op grond van de False Statements Act (wet valse verklaringen) (18 U.S.C. § 1001).

([83]) Tijdens de tweede jaarlijkse evaluatie van het privacyschild deelde het ministerie van Handel mee dat het bij 100 organisaties steekproeven had uitgevoerd en in 21 gevallen nalevingsvragenlijsten had verstuurd (waarna de geconstateerde problemen werden verholpen), zie Werkdocument van de diensten van de Commissie SWD (2018) 497 final, blz. 9. Evenzo meldde het ministerie van Handel tijdens de derde jaarlijkse evaluatie van het privacyschild dat het drie incidenten had ontdekt via zijn monitoring van openbare verslagen en de praktijk was begonnen om maandelijks steekproefsgewijs 30 bedrijven te controleren, wat in 28 % van de gevallen leidde tot follow-up met nalevingsvragenlijsten (waarna de ontdekte problemen onmiddellijk werden verholpen of, in drie gevallen, werden opgelost na een waarschuwingsbrief), zie Werkdocument van de diensten van de Commissie SWD (2019) 495 final, blz. 8.

([84]) Bijlage I, hoofdstuk III, punt 11, g). Van aanhoudende niet-naleving is met name sprake wanneer een organisatie weigert te voldoen aan een definitieve beslissing van een instantie voor zelfregulering op het gebied van privacy, onafhankelijke geschillenbeslechting of handhaving.

([85]) Bijlage I, hoofdstuk III, punt 6, f).

([86]) Bijlage III, hoofdstuk "Zoeken naar en aanpakken van valse beweringen aangaande deelname".

([87]) *Zie vorige voetnoot*.

([88]) *Zie vorige voetnoot*.

([89]) *Zie vorige voetnoot*.

([90]) In het kader van het privacyschild meldde het ministerie van Handel tijdens de derde jaarlijkse evaluatie van het kader dat het 669 gevallen van valse beweringen van deelname had vastgesteld (tussen oktober 2018 en oktober 2019), waarvan de meeste werden opgelost na de waarschuwingsbrief van het ministerie van Handel; 143 gevallen werden doorverwezen naar de FTC (zie overweging 62). Zie Werkdocument van de diensten van de Commissie SWD (2019) 495 final, blz. 10.

2.3.4 ***Handhaving***

(58) Om ervoor te zorgen dat in de praktijk een passend niveau van bescherming van persoonsgegevens wordt gewaarborgd, moet er worden voorzien in een onafhankelijke toezichthoudende autoriteit met bevoegdheden tot monitoring en handhaving van de naleving van de gegevensbeschermingsvoorschriften.

(59) EU-VS-DPF-organisaties moeten onderworpen zijn aan de jurisdictie van de bevoegde Amerikaanse autoriteiten — de FTC en het ministerie van Vervoer — die over de nodige onderzoeks- en handhavingsbevoegdheden beschikken om de naleving van de beginselen daadwerkelijk te waarborgen ([91]).

(60) De FTC is een onafhankelijke instantie die bestaat uit vijf commissarissen, die door de president worden benoemd met het advies en de instemming van de Senaat ([92]). De commissarissen worden benoemd voor een periode van zeven jaar en kunnen alleen door de president worden ontslagen wegens inefficiëntie, plichtsverzuim of ambtsmisdrijven. De FTC mag niet meer dan drie commissarissen van dezelfde politieke partij hebben en de commissarissen mogen tijdens hun benoeming geen andere zakelijke activiteiten, beroepen of functies uitoefenen.

(61) De FTC kan een onderzoek instellen naar de naleving van de beginselen, alsook naar valse beweringen over de naleving van de beginselen of de deelname aan het EU-VS-DPF door organisaties die niet langer op de DPF-lijst staan of die nooit zijn gecertificeerd ([93]). De FTC kan naleving afdwingen door administratieve of federale rechterlijke bevelen te vragen (met inbegrip van *consent orders* die via schikkingen tot stand zijn gekomen) ([94]) voor voorlopige of permanente bevelen of andere rechtsmiddelen, en zal systematisch toezien op de naleving van dergelijke bevelen ([95]). In geval van niet-naleving van dergelijke bevelen door organisaties kan de FTC civielrechtelijke sancties en ander herstel vorderen, onder meer voor door de onrechtmatige gedraging veroorzaakte schade. Elk tegen een EU-VS-DPF-organisatie uitgevaardigd consent order zal bepalingen inzake zelfrapportage bevatten ([96]) en organisaties zullen alle relevante delen over het EU-VS-DPF van bij de FTC ingediende nalevings- of beoordelingsverslagen openbaar moeten maken. Ten slotte zal de FTC online een lijst bijhouden van de organisaties waartegen bevelen van de FTC of een rechterlijke instantie zijn uitgevaardigd in zaken betreffende het EU-VS-DPF ([97]).

(62) Met betrekking tot het privacyschild heeft de FTC in ongeveer 22 gevallen handhavingsmaatregelen genomen, zowel met betrekking tot schendingen van specifieke vereisten van het kader (bv. nalaten om aan het ministerie van Handel te bevestigen dat de organisatie de privacyschildbeschermingen bleef toepassen nadat zij het kader had verlaten, nalaten om door middel van een zelfbeoordeling of een externe nalevingscontrole na te gaan of de organisatie aan het kader voldeed) ([98]) als met betrekking tot valse beweringen over deelname aan het kader (bv. door organisaties die niet de nodige stappen ondernamen om een certificering te verkrijgen, of hun certificering lieten verlopen maar een verkeerde voorstelling gaven van hun verdere deelname) ([99]). Deze handhavingsactie vloeide onder meer voort uit het proactieve gebruik van administratieve dwangbevelen om bij bepaalde deelnemers aan het privacyschild materiaal te verkrijgen om te controleren op materiële schendingen van de privacyschildverplichtingen ([100]).

([91]) Een EU-VS-DPF-organisatie moet in het openbaar verklaren dat zij zich ertoe verbindt de beginselen na te leven, overeenkomstig die beginselen haar privacybeleid openbaar maken en dat beleid volledig uitvoeren. Tegen niet-naleving kan worden opgetreden op grond van sectie 5 van de *FTC Act*, die oneerlijke en misleidende handelingen verbiedt in of met invloed op de handel (15 U.S.C. § 45) en 49 U.S.C. § 41712 die een luchtvaartmaatschappij of reisbureau verbiedt zich in te laten met oneerlijke of misleidende praktijken in het luchtvervoer of de verkoop van luchtvervoer.

([92]) 15 U.S.C. § 41.

([93]) Bijlage IV.

([94]) Volgens de informatie van de FTC is zij niet bevoegd om ter plekke inspecties op het gebied van privacybescherming te verrichten. Zij is echter bevoegd om organisaties te verplichten tot overlegging van documenten en getuigenverklaringen (zie sectie 20 van de FTC Act) en kan zich tot rechterlijke instanties wenden om dergelijke bevelen te doen handhaven in geval van niet-naleving.

([95]) Zie bijlage IV, hoofdstuk "Verzoek om en toezicht op bevelen".

([96]) Een bevel van de FTC of een rechterlijke instantie kan ondernemingen ertoe verplichten privacyprogramma's te implementeren en regelmatig nalevingsverslagen of onafhankelijke beoordelingen door derden van die programma's ter beschikking te stellen van de FTC.

([97]) Bijlage IV, hoofdstuk "Verzoek om en toezicht op bevelen".

([98]) Werkdocument van de diensten van de Commissie SWD (2019) 495 final, blz. 11.

([99]) Zie de lijst van zaken op de website van de FTC, beschikbaar op https://www.ftc.gov/business-guidance/privacy-security/privacy-shield. Zie ook Werkdocument van de diensten van de Commissie SWD (2017) 344 final, blz. 17; Werkdocument van de diensten van de Commissie SWD (2018) 497 final, blz. 12 en Werkdocument van de diensten van de Commissie SWD (2019) 495 final, blz. 11.

([100]) Zie bv. de opmerkingen van voorzitter Joseph Simons bij de tweede jaarlijkse evaluatie van het privacyschild (ftc.gov).

(63) Meer in het algemeen heeft de FTC de voorbije jaren handhavingsmaatregelen genomen in een aantal zaken betreffende de naleving van specifieke vereisten voor de bescherming van gegevens waarin ook is voorzien in het kader van het EU-VS-DPF, bv. in verband met de beginselen van doelbinding en bewaring van gegevens ([101]), minimale verwerking van gegevens ([102]), gegevensbeveiliging ([103]) en nauwkeurigheid van gegevens ([104]).

(64) Het ministerie van Vervoer heeft de exclusieve bevoegdheid om de privacypraktijken van luchtvaartmaatschappijen te reguleren en deelt rechtsbevoegdheid met de FTC met betrekking tot de privacypraktijken van reisbureaus bij de verkoop van luchtvervoer. De functionarissen van het ministerie van Vervoer proberen eerst een schikking te treffen en als dat niet mogelijk is, kunnen zij een handhavingsprocedure inleiden met een hoorzitting voor een bestuursrechter van het ministerie van Vervoer die bevoegd is om administratieve bevelen uit te vaardigen en civiele sancties op te leggen ([105]). Bestuursrechters genieten op grond van de Administrative Procedure Act (wet bestuursrechtelijke procedure, hierna "APA") verschillende beschermingsmaatregelen om hun onafhankelijkheid en onpartijdigheid te waarborgen. Zij kunnen bijvoorbeeld alleen om gegronde redenen worden ontslagen; worden bij beurtrol aan zaken toegewezen; mogen geen taken vervullen die onverenigbaar zijn met hun taken en verantwoordelijkheden als bestuursrechter; staan niet onder toezicht van het onderzoeksteam van de autoriteit waarbij zij in dienst zijn (in dit geval het ministerie van Vervoer); en moeten hun rechtsprekende/handhavende functie onpartijdig uitoefenen ([106]). Het ministerie van Vervoer heeft toegezegd toezicht te houden op handhavingsbevelen en ervoor te zorgen dat bevelen die voortvloeien uit EU-VS-DPF-zaken beschikbaar zijn op zijn website ([107]).

2.4 **Verhaalmechanismemogelijkheden**

(65) Om een passende bescherming en vooral de handhaving van individuele rechten te waarborgen, moeten aan de betrokkene doeltreffende administratieve en gerechtelijke verhaalmechanismemogelijkheden worden verstrekt.

(66) Het EU-VS-DPF vereist in het beginsel van verhaal, handhaving en aansprakelijkheid dat organisaties natuurlijke personen die door de niet-naleving worden getroffen, verhaalmechanismen bieden en dus voor betrokkenen uit de Unie de mogelijkheid bieden een klacht in te dienen betreffende niet-naleving door EU-VS-DPF-organisaties en die klachten opgelost te zien, indien nodig door een beslissing die een doeltreffend herstel biedt ([108]). Als onderdeel van hun certificering moeten organisaties voldoen aan de vereisten van dit beginsel door doeltreffende en direct beschikbare onafhankelijke verhaalmechanismen aan te bieden waarmee de klachten van een natuurlijke persoon en geschillen kunnen worden onderzocht en snel worden opgelost zonder kosten voor de natuurlijke persoon ([109]).

([101]) Zie bv. het bevel van de FTC in de zaak Drizly, LLC., waarbij de onderneming (1) alle verzamelde persoonsgegevens moet vernietigen die niet noodzakelijk zijn voor het verstrekken van producten of diensten aan consumenten, (2) geen persoonsgegevens mag verzamelen of opslaan tenzij dit nodig is voor specifieke doeleinden die zijn uiteengezet in een bewaarschema.

([102]) Zie bv. het bevel van de FTC in de zaak CafePress (24 maart 2022) waarin onder meer werd geëist dat de onderneming het aantal verzamelde gegevens zoveel mogelijk beperkte.

([103]) Zie bv. de handhavingsmaatregel van de FTC in de zaken Drizzly, LLC en CafePress, waar zij eiste dat de betrokken ondernemingen een speciaal daartoe bestemd beveiligingsprogramma of specifieke beveiligingsmaatregelen zouden invoeren. Zie voor gegevensinbreuken ook het bevel van de FTC van 27 januari 2023 in de zaak Chegg, de schikking in de zaak Equifax in 2019 (https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach).

([104]) Zie bv. de zaak RealPage, Inc (16 oktober 2018), waar de FTC uit hoofde van de FCRA handhavingsmaatregelen trof tegen een onderneming die huurders doorlichtte en daarbij achtergrondverslagen over natuurlijke personen verstrekte aan vastgoedeigenaren en vastgoedbeheermaatschappijen op basis van gegevens uit huurgeschiedenissen, gegevens uit openbare registers (met inbegrip van strafregisters en verslagen van uitzettingen) en kredietgegevens, die werden gebruikt om te bepalen of iemand voor huisvesting in aanmerking kwam. De FTC kwam tot de vaststelling dat de onderneming geen redelijke maatregelen had getroffen om de nauwkeurigheid te waarborgen van de gegevens die zij op basis van haar instrument voor geautomatiseerde besluitvorming verstrekte.

([105]) Zie bijlage V, hoofdstuk "Handhavingspraktijken".

([106]) Zie 5 U.S.C. §§ 3105, 7521(a), 554(d) en 556(b)(3).

([107]) Bijlage V, hoofdstuk "Toezicht op uitvoering en openbaarmaking van handhavingsbevelen inzake schendingen van het EU-VS-DPF".

([108]) Bijlage I, hoofdstuk II, punt 7.

([109]) Bijlage I, hoofdstuk III, punt 11.

(67) Organisaties mogen onafhankelijke verhaalmechanismen kiezen in hetzij de Unie hetzij de Verenigde Staten. Zoals in overweging 73 nader wordt toegelicht, omvat dit de mogelijkheid om zich vrijwillig tot samenwerking met de gegevensbeschermingsautoriteiten van de EU te verbinden. Wanneer organisaties personeelsgegevens verwerken, is een dergelijke verbintenis tot samenwerking met de gegevensbeschermingsautoriteiten van de EU verplicht. Andere alternatieven zijn onafhankelijke alternatieve geschillenbeslechting of door de particuliere sector ontwikkelde privacyprogramma's die de beginselen in hun regels hebben opgenomen. Die programma's moeten doeltreffende handhavingsmechanismen omvatten overeenkomstig de vereisten van het beginsel van verhaal, handhaving en aansprakelijkheid.

(68) Het EU-VS-DPF biedt betrokkenen bijgevolg een aantal mogelijkheden om hun rechten te doen handhaven, klachten in te dienen betreffende niet-naleving door EU-VS-DPF-organisaties en hun klachten opgelost te zien, indien nodig met een beslissing die een doeltreffend herstel biedt. Natuurlijke personen kunnen een klacht direct bij een organisatie indienen, bij een onafhankelijke geschillenbeslechtingsinstantie die door de organisatie is aangewezen, bij nationale gegevensbeschermingsautoriteiten, het ministerie van Handel of bij de FTC. In gevallen waarin hun klachten niet zijn opgelost door een van deze verhaalmechanisme- of handhavingsmechanismen, hebben natuurlijke personen ook het recht om bindende arbitrage in te roepen (bijlage I bij bijlage I bij dit besluit). Behalve voor het arbitragepanel, waarvoor bepaalde rechtsmiddelen moeten zijn uitgeput voordat het kan worden ingeroepen, staat het natuurlijke personen vrij om een of alle verhaalmechanismen van hun keuze te gebruiken, en zijn zij niet verplicht om voor het ene of het andere mechanisme te kiezen of een bepaalde volgorde te eerbiedigen.

(69) Ten eerste kunnen betrokkenen uit de Unie gevallen van niet-naleving van de beginselen aankaarten via rechtstreekse contacten met de EU-VS-DPF-organisaties ([110]). Om die klachten gemakkelijk op te lossen, moet de organisatie een doeltreffend verhaalmechanisme invoeren om klachten te behandelen. Het privacybeleid van een organisatie moet dus duidelijke informatie voor natuurlijke personen bevatten over een contactpunt, binnen of buiten de organisatie, dat klachten zal behandelen (met inbegrip van relevante vestigingen in de Unie die op vragen of klachten kunnen reageren) en over de aangewezen onafhankelijke geschillenbeslechtingsinstantie (zie overweging 70). Na ontvangst van een klacht van een natuurlijke persoon, direct van de natuurlijke persoon of via het ministerie van Handel na verwijzing door een gegevensbeschermingsautoriteit, moet de organisatie de betrokkene uit de Unie een antwoord geven binnen een termijn van 45 dagen ([111]). Daarnaast moeten organisaties onmiddellijk reageren op vragen en andere informatieverzoeken van het ministerie van Handel ([112]) of van een gegevensbeschermingsautoriteit (wanneer de organisatie zich verbonden heeft tot samenwerking met de gegevensbeschermingsautoriteiten) betreffende hun naleving van de beginselen.

(70) Ten tweede kunnen natuurlijke personen een klacht ook direct indienen bij de onafhankelijke geschillenbeslechtingsinstantie (in de Verenigde Staten of in de Unie) die door een organisatie is aangewezen om individuele klachten te onderzoeken en te beslechten (tenzij deze duidelijk ongegrond of niet ernstig zijn) en kosteloos te voorzien in passend verhaal voor de natuurlijke persoon ([113]). De sancties en het herstel die door een dergelijke instantie worden opgelegd, moeten zwaar genoeg zijn om de naleving van de beginselen door organisaties te waarborgen en erin voorzien dat de gevolgen van de niet-naleving door de organisatie ongedaan worden gemaakt of worden gecorrigeerd en, afhankelijk van de omstandigheden, dat de verdere verwerking van de desbetreffende persoonsgegevens wordt beëindigd en/of dat deze worden gewist, en dat geconstateerde gevallen van niet-naleving worden bekendgemaakt ([114]). De door een organisatie aangewezen onafhankelijke geschillenbeslechtingsinstanties moeten op hun openbare websites relevante informatie verstrekken over het EU-VS-DPF en de diensten die zij in het kader daarvan verlenen ([115]). Zij moeten elk jaar een jaarverslag publiceren met daarin geaggregeerde statistieken met betrekking tot deze diensten ([116]).

([110]) Bijlage I, hoofdstuk III, punt 11, d), i).
([111]) Bijlage I, hoofdstuk III, punt 11, d), i).
([112]) Dit is de instantie die is aangewezen door het panel van gegevensbeschermingsautoriteiten waarin is voorzien in het aanvullende beginsel inzake de rol van de gegevensbeschermingsautoriteiten (bijlage I, hoofdstuk III, punt 5).
([113]) Bijlage I, hoofdstuk III, punt 11, d).
([114]) Bijlage I, hoofdstuk II, punt 7 en hoofdstuk III, punt 11, e).
([115]) Bijlage I, hoofdstuk III, punt 11, d), ii).
([116]) Het jaarverslag moet het volgende bevatten: 1) het totale aantal tijdens het verslagjaar ontvangen klachten in verband met het EU-VS-DPF; 2) de soorten ontvangen klachten; 3) maatstaven inzake de kwaliteit van de geschillenbeslechting, zoals de tijd die met de verwerking van klachten gemoeid was; en 4) de resultaten van de ontvangen klachten, met name het aantal en de soorten genomen maatregelen of opgelegde sancties.

(71) In het kader van zijn nalevingscontroles zal het ministerie van Handel controleren of alle EU-VS-DPF-organisaties daadwerkelijk geregistreerd staan bij de onafhankelijke verhaalmechanismen waarbij zij beweren geregistreerd te staan ([117]). Zowel de organisaties als de verantwoordelijke onafhankelijke verhaalmechanismen moeten onmiddellijk reageren op vragen en informatieverzoeken van het ministerie van Handel in verband met het EU-VS-DPF. Het ministerie van Handel zal met onafhankelijke verhaalmechanismen samenwerken om na te gaan of zij op hun websites informatie verstrekken over de beginselen en de diensten die zij in het kader van het EU-VS-DPF verlenen, en of zij jaarverslagen publiceren ([118]).

(72) Wanneer de organisatie de uitspraak van een geschillenbeslechtingsinstantie of zelfregulerende instantie niet naleeft, moet deze laatste het ministerie van Handel en de FTC (of een andere Amerikaanse autoriteit die bevoegd is om niet-naleving door de organisatie te onderzoeken) of een bevoegde rechterlijke instantie van deze niet-naleving in kennis stellen ([119]). Indien een organisatie weigert een definitieve uitspraak van een geschillenbeslechtingsinstantie, een zelfregulerende instantie of een overheidsinstantie na te leven, of indien een dergelijke instantie vaststelt dat een organisatie frequent de beginselen niet naleeft, kan dit als een permanente niet-naleving worden beschouwd, die ertoe leidt dat het ministerie van Handel de organisatie uit de DPF-lijst verwijdert, doch pas nadat het de organisatie daarvan 30 dagen van tevoren in kennis heeft gesteld en de kans heeft gegeven om te reageren ([120]). Indien de organisatie na verwijdering uit de lijst blijft beweren dat zij het keurmerk van het EU-VS-DPF heeft, zal het ministerie van Handel dit verwijzen naar de FTC of een andere handhavingsinstantie ([121]).

(73) Ten derde kunnen natuurlijke personen hun klachten ook indienen bij een nationale gegevensbeschermingsautoriteit in de Unie, die gebruik kan maken van haar corrigerende en onderzoeksbevoegdheden uit hoofde van Verordening (EU) 2016/679. Organisaties moeten medewerking verlenen aan het onderzoek en de oplossing van een klacht door een gegevensbeschermingsautoriteit wanneer het gaat om 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 ([122]). Organisaties moeten met name reageren op vragen, gevolg geven aan het advies van de gegevensbeschermingsautoriteit, daaronder begrepen corrigerende of compenserende maatregelen, en de gegevensbeschermingsautoriteit schriftelijk bevestigen dat dergelijke maatregelen zijn genomen ([123]). Wanneer het door de gegevensbeschermingsautoriteit verstrekte advies niet wordt nageleefd, zal de gegevensbeschermingsautoriteit de zaak doorverwijzen naar het ministerie van Handel (dat organisaties van de EU-VS-DPF-lijst kan verwijderen) of, met het oog op mogelijke handhavingsmaatregelen, naar de FTC of het ministerie van Vervoer (tegen niet samenwerken met de gegevensbeschermingsautoriteiten of niet-naleving van de beginselen kan uit hoofde van het Amerikaanse recht actie worden ingesteld) ([124]).

(74) Om de samenwerking voor een doeltreffende behandeling van klachten te vergemakkelijken, hebben zowel het ministerie van Handel als de FTC een speciaal contactpunt opgericht dat verantwoordelijk is voor de rechtstreekse contacten met de gegevensbeschermingsautoriteiten ([125]). Deze contactpunten helpen gegevensbeschermingsautoriteiten bij vragen over de naleving van de beginselen door een organisatie.

(75) Het advies van de gegevensbeschermingsautoriteiten ([126]) wordt uitgebracht nadat beide partijen in het geschil een redelijke kans hebben gekregen om opmerkingen in te dienen en alle gewenste bewijzen te leveren. Het panel zal het advies zo snel geven als een eerlijke rechtsgang toestaat en in de regel binnen 60 dagen na ontvangst van een klacht ([127]). Als een organisatie niet binnen 25 dagen nadat het advies is uitgebracht, gevolg geeft aan dit advies en hiervoor geen bevredigende verklaring geeft, zal het panel kennisgeven van zijn voornemen om de zaak voor te leggen aan de FTC (of een andere bevoegde Amerikaanse handhavingsinstantie), of om te concluderen dat de verbintenis tot samenwerking ernstig is geschonden. In het eerste geval kan dit leiden tot handhavingsmaatregelen

([117]) Bijlage III, hoofdstuk "De inachtneming van de vereisten inzake zelfcertificering controleren".
([118]) Zie bijlage III, hoofdstuk "Samenwerking faciliteren met instanties voor alternatieve geschillenbeslechting die diensten in verband met de beginselen verlenen". Zie ook bijlage I, hoofdstuk III, punt 11, d), ii) en iii).
([119]) Zie bijlage I, hoofdstuk III, punt 11, e).
([120]) Zie bijlage II, hoofdstuk III, punt 11, g), met name ii) en iii).
([121]) Zie bijlage III, hoofdstuk "Zoeken naar en aanpakken van valse beweringen aangaande deelname".
([122]) Bijlage I, hoofdstuk II, punt 7, b).
([123]) Bijlage I, hoofdstuk III, punt 5.
([124]) Bijlage I, hoofdstuk III, punt 5, c), ii).
([125]) Bijlage III (zie hoofdstuk "Samenwerking met de gegevensbeschermingsautoriteiten faciliteren") en bijlage IV (zie de hoofdstukken "Het geven van prioriteit aan verwijzingen en onderzoeken" en "Handhavingssamenwerking met de gegevensbeschermingsautoriteiten in de EU").
([126]) De procedureregels van het informele panel van gegevensbeschermingsautoriteiten moeten door de gegevensbeschermingsautoriteiten worden vastgesteld op grond van hun bevoegdheid om hun werkzaamheden te organiseren en met elkaar samen te werken.
([127]) Bijlage I, hoofdstuk III, punt 5, c), i).

op grond van sectie 5 van de FTC Act (of andere soortgelijke wetten) ([128]). In het tweede geval zal het panel het ministerie van Handel hiervan op de hoogte brengen, dat de weigering van de organisatie als een permanente niet-naleving zal beschouwen, die ertoe zal leiden dat de organisatie uit de DPF-lijst wordt verwijderd.

(76) Indien de gegevensbeschermingsautoriteit waarbij de klacht is ingediend, geen of ontoereikende maatregelen heeft genomen om een klacht te behandelen, heeft de individuele klager de mogelijkheid om dergelijk (niet-)optreden aan te vechten bij de nationale rechter van de respectieve EU-lidstaat.

(77) Natuurlijke personen kunnen ook klachten bij de gegevensbeschermingsautoriteiten indienen wanneer het panel van gegevensbeschermingsautoriteiten niet is aangewezen als de geschillenbeslechtingsinstantie van een organisatie. In die gevallen kan de gegevensbeschermingsautoriteit die klachten verwijzen naar hetzij het ministerie van Handel hetzij de FTC. Om de samenwerking inzake aangelegenheden met betrekking tot individuele klachten en niet-naleving door EU-VS-DPF-organisaties te vergemakkelijken en te vergroten, zal het ministerie van Handel een specifiek contactpunt instellen dat als verbindingspunt fungeert en bijdraagt aan onderzoeken van gegevensbeschermingsautoriteiten met betrekking tot de naleving van de beginselen door een organisatie ([129]). Evenzo heeft de FTC toegezegd een speciaal contactpunt in te stellen ([130]).

(78) Ten vierde heeft het ministerie van Handel toegezegd klachten met betrekking tot de niet-naleving van de beginselen door een organisatie te ontvangen en te controleren, en zich maximaal in te spannen om die op te lossen ([131]). Hiertoe voorziet het ministerie van Handel in speciale procedures voor gegevensbeschermingsautoriteiten om klachten te verwijzen naar een specifiek contactpunt, die te volgen en contact op te nemen met organisaties om de oplossing ervan te vergemakkelijken ([132]). Om de verwerking van individuele klachten te bespoedigen, houdt het contactpunt rechtstreeks contact met de respectieve gegevensbeschermingsautoriteit inzake nalevingskwesties en stelt deze in het bijzonder binnen een termijn van ten hoogste 90 dagen na de verwijzing in kennis van de status van klachten ([133]). Hierdoor kunnen betrokkenen klachten over niet-naleving door EU-VS-DPF-organisaties rechtstreeks bij hun nationale gegevensbeschermingsautoriteit indienen en laten toezenden aan het ministerie van Handel als de Amerikaanse autoriteit die het EU-VS-DPF beheert.

(79) Wanneer het ministerie van Handel op basis van zijn ambtshalve controles, klachten of andere informatie concludeert dat een organisatie de beginselen permanent niet heeft nageleefd, kan het die organisatie uit de DPF-lijst verwijderen ([134]). De weigering om een definitieve uitspraak van een zelfregulerende instantie, een onafhankelijke geschillenbeslechtingsinstantie of een overheidsinstantie, waaronder een gegevensbeschermingsautoriteit, na te leven, wordt als een permanente niet-naleving beschouwd ([135]).

(80) Ten vijfde moet een EU-VS-DPF-organisatie onderworpen zijn aan de jurisdictie van de Amerikaanse autoriteiten, met name de FTC ([136]), die over de nodige onderzoeks- en handhavingsbevoegdheden beschikken om de naleving van de beginselen daadwerkelijk te waarborgen. De FTC geeft prioriteit aan zaken in verband met niet-naleving van de beginselen die door onafhankelijke geschillenbeslechtingsinstanties of zelfregulerende organisaties, het ministerie van Handel en gegevensbeschermingsautoriteiten (ambtshalve of naar aanleiding van een klacht) naar haar zijn verwezen om te bepalen of sectie 5 van de FTC Act geschonden is ([137]). De FTC heeft toegezegd een gestandaardiseerde verwijzingsprocedure tot stand te brengen, een contactpunt aan te wijzen voor verwijzingen van gegevensbeschermingsautoriteiten en informatie over verwijzingen uit te wisselen. Daarnaast kan de FTC rechtstreeks door natuurlijke personen ingediende klachten aanvaarden en op eigen initiatief onderzoeken van het EU-VS-DPF verrichten, met name als onderdeel van haar ruimere onderzoeken van privacykwesties.

([128]) Bijlage I, hoofdstuk III, punt 5, c), ii).
([129]) Zie bijlage III, hoofdstuk "Samenwerking met de gegevensbeschermingsautoriteiten faciliteren".
([130]) Zie bijlage IV, de hoofdstukken "Het geven van prioriteit aan verwijzingen en onderzoeken" en "Handhavingssamenwerking met de gegevensbeschermingsautoriteiten in de EU".
([131]) Bijlage III, zie bv. het hoofdstuk "Samenwerking met de gegevensbeschermingsautoriteiten faciliteren".
([132]) Bijlage I, hoofdstuk II, punt 7, e), en bijlage III, hoofdstuk "Samenwerking met de gegevensbeschermingsautoriteiten faciliteren".
([133]) *Zie vorige voetnoot.*
([134]) Bijlage I, hoofdstuk III, punt 11, g).
([135]) Bijlage I, hoofdstuk III, punt 11, g).
([136]) Een EU-VS-DPF-organisatie moet in het openbaar verklaren dat zij zich ertoe verbindt de beginselen na te leven, overeenkomstig die beginselen haar privacybeleid openbaar maken en dat beleid volledig uitvoeren. Tegen niet-naleving kan worden opgetreden op grond van sectie 5 van de FTC Act, die oneerlijke en misleidende handelingen verbiedt in of met invloed op de handel.
([137]) Zie ook de soortgelijke verbintenissen van het ministerie van Vervoer, bijlage V.

(81) Ten zesde kan de betrokkene uit de Unie, als verhaalmechanisme „in laatste instantie" ingeval zijn klacht door geen van de andere beschikbare verhaalmechanismen naar tevredenheid is opgelost, bindende arbitrage door het panel van het EU-VS-kader voor gegevensbescherming (hierna "EU-VS-DPF-panel" genoemd) inroepenEU de inroepen ([138]). Organisaties moeten natuurlijke personen informeren over de mogelijkheid om bindende arbitrage in te roepen en zij moeten reageren zodra een natuurlijke persoon die optie inroept door een kennisgeving aan de betrokken organisatie ([139]).

(82) Dit EU-VS-DPF-panel bestaat uit een groep van ten minste tien arbiters die zijn aangewezen door het ministerie van Handel en de Commissie op basis van hun onafhankelijkheid, integriteit en ervaring op het gebied van de Amerikaanse privacywetgeving en de Uniewetgeving inzake gegevensbescherming. Voor elk individueel geschil selecteren de partijen uit deze groep een panel van één of drie ([140]) arbiters.

(83) Het *International Centre for Dispute Resolution* (ICDR), de internationale afdeling van de *American Arbitration Association* (AAA), is door het ministerie van Handel geselecteerd om de arbitrages te beheren. Op de procedures voor het EU-VS-DPF-panel zijn een reeks overeengekomen arbitrageregels en een gedragscode voor aangewezen arbiters van toepassing. De website van het ICDR-AAA verstrekt duidelijke en beknopte informatie aan natuurlijke personen over het arbitragemechanisme en de procedure om arbitrage aan te vragen.

(84) De tussen het ministerie van Handel en de Commissie overeengekomen arbitrageregels vormen een aanvulling op het EU-VS-DPF, dat verscheidene kenmerken bevat die de toegankelijkheid van dit mechanisme voor de betrokkenen uit de Unie vergroten: i) bij de voorbereiding van een geschil voor het panel mag de betrokkene worden bijgestaan door zijn of haar nationale gegevensbeschermingsautoriteit; ii) hoewel de arbitrage in de Verenigde Staten zal plaatsvinden, kunnen betrokkenen uit de Unie ervoor kiezen hieraan deel te nemen per video- of telefoonconferentie, wat zonder kosten voor de natuurlijke persoon wordt aangeboden; iii) hoewel de taal van de arbitrage in de regel Engels zal zijn, zullen normaal gezien vertolking ter zitting en vertaling op met redenen omkleed verzoek zonder kosten voor de betrokkene worden aangeboden; iv) ten slotte, hoewel elke partij haar eigen advocaatkosten moet dragen indien zij voor het panel door een advocaat wordt vertegenwoordigd, zal het ministerie van Handel een fonds oprichten waarin jaarlijkse bijdragen van de EU-VS-DPF-organisaties worden gestort en waarmee de kosten van de arbitrageprocedure worden gedekt tot maximumbedragen die door de Amerikaanse autoriteiten in overleg met de Commissie worden bepaald ([141]).

(85) Het EU-VS-DPF-panel is bevoegd om individuspecifieke, niet-monetaire billijke schadeloosstelling ([142]) op te leggen die noodzakelijk is om de niet-naleving van de beginselen te verhelpen. Hoewel het panel in zijn uitspraak rekening houdt met het andere herstel dat reeds via andere mechanismen van het EU-VS-DPF is verkregen, kunnen natuurlijke personen nog steeds arbitrage inroepen als zij dat andere herstel ontoereikend achten. Hierdoor zullen betrokkenen uit de Unie arbitrage kunnen inroepen in alle gevallen waarin hun klachten niet naar tevredenheid zijn opgelost door de maatregelen die de EU-VS-DPF-organisaties, onafhankelijke verhaalmechanismen of de bevoegde Amerikaanse autoriteiten (bijvoorbeeld de FTC) hebben genomen of net niet hebben genomen. Arbitrage kan niet worden ingeroepen als een gegevensbeschermingsautoriteit wettelijk bevoegd is om de betrokken klacht met betrekking tot de EU-VS-DPF-organisatie te behandelen, namelijk in die gevallen waarin de organisatie verplicht is om samen te werken met en gevolg te geven aan het advies van de gegevensbeschermingsautoriteiten met betrekking tot de verwerking van in het kader van een arbeidsverhouding verzamelde personeelsgegevens, of zich daar vrijwillig toe heeft verbonden. Natuurlijke personen kunnen de arbitragebeslissing in de Amerikaanse rechterlijke instanties doen handhaven op grond van de Federal Arbitration Act, waardoor een rechtsmiddel gewaarborgd is indien een organisatie de beslissing niet naleeft.

([138]) Zie bijlage I bij bijlage I, "Arbitragemodel".
([139]) Zie bijlage I, hoofdstuk II, punt 1, a), xi) en hoofdstuk II, punt 7, c).
([140]) Het aantal arbiters in het panel zal door de partijen worden overeengekomen.
([141]) Bijlage I bij bijlage I, hoofdstuk G.6.
([142]) Natuurlijke personen kunnen in een arbitrageprocedure geen schadevergoeding vorderen, maar als arbitrage wordt ingeroepen, blijft de optie om voor de gewone Amerikaanse rechterlijke instanties schadevergoeding te vorderen, bestaan.

(86) Ten zevende zijn er, wanneer een organisatie haar verbintenis om de beginselen en het gepubliceerde privacybeleid na te leven niet nakomt, volgens het Amerikaanse recht aanvullende rechtsmiddelen beschikbaar, onder meer om schadevergoeding te verkrijgen. Zo kunnen natuurlijke personen onder bepaalde voorwaarden bij de rechter verhaal halen (met inbegrip van schadevergoeding) op grond van de consumentenwetgeving van de Amerikaanse staten in geval van een bedrieglijke voorstelling van zaken, oneerlijke of misleidende handelingen of praktijken ([143]), en op grond van het recht inzake onrechtmatige daad (met name op grond van de onrechtmatige daden van inbreuk op de persoonlijke levenssfeer ([144]), toe-eigening van naam of gelijkenis ([145]) en openbaarmaking van privéfeiten ([146])).

(87) De verschillende hierboven beschreven verhaalmechanismemogelijkheden zorgen er samen voor dat elke klacht in verband met niet-naleving van het EU-VS-DPF door gecertificeerde organisaties daadwerkelijk zal worden beoordeeld en verholpen.

3. TOEGANG TOT EN GEBRUIK VAN UIT DE EUROPESE UNIE DOORGEGEVEN PERSOONSGEGEVENS DOOR OVERHEIDSINSTANTIES IN DE VERENIGDE STATEN

(88) De Commissie heeft ook de beperkingen en waarborgen beoordeeld, inclusief de mechanismen voor toezicht en individueel verhaal in het recht van de Verenigde Staten met betrekking tot de verzameling en het daaropvolgende gebruik van persoonsgegevens die door Amerikaanse overheidsinstanties in het openbaar belang, met name voor de handhaving van het strafrecht en de nationale veiligheid, worden doorgegeven aan verwerkingsverantwoordelijken en verwerkers in de VS (overheidstoegang) ([147]). Bij de beoordeling van de vraag of de voorwaarden waaronder overheidstoegang tot gegevens die op grond van dit besluit aan de Verenigde Staten worden doorgegeven "in feite overeenkomend" zijn met artikel 45, lid 1, van Verordening (EU) 2016/679, zoals uitgelegd door het Hof van Justitie in het licht van het Handvest van de grondrechten, heeft de Commissie met name rekening gehouden met de volgende criteria.

(89) In het bijzonder moet elke beperking van het recht op bescherming van persoonsgegevens bij wet worden geregeld en moet de rechtsgrondslag die de aantasting van een dergelijk recht mogelijk maakt, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht bepalen ([148]). Bovendien moet, om te voldoen aan het evenredigheidsvereiste, dat inhoudt dat afwijkingen en beperkingen van de bescherming van persoonsgegevens slechts van toepassing mogen zijn voor zover zulks in een democratische samenleving strikt noodzakelijk is om specifieke doelstellingen van algemeen belang te verwezenlijken die gelijkwaardig zijn aan die welke door de Unie worden erkend, deze rechtsgrondslag duidelijke en nauwkeurige regels betreffende de werkingssfeer en de toepassing van de betrokken maatregelen vaststellen en minimumwaarborgen opleggen, opdat de personen wier gegevens zijn doorgegeven, over voldoende waarborgen beschikken om hun persoonsgegevens doeltreffend te beschermen tegen het risico van misbruik ([149]). Deze regels en waarborgen moeten bovendien juridisch bindend en

([143]) Zie bv. de consumentenbeschermingswetten van de staat Californië (Cal. Civ. Code §§ 1750 – 1785 (West) Consumers Legal Remedies Act); District of Columbia (D.C. Code §§ 28-3901); Florida (Fla. Stat. §§ 501.201 – 501.213, Deceptive and Unfair Trade Practices Act); Illinois (815 Ill. Comp. Stat. 505/1 – 505/12, Consumer Fraud and Deceptive Business Practices Act); Pennsylvania (73 Pa. Stat. Ann. §§ 201-1 – 201-9.3 (West) Unfair Trade Practices and Consumer Protection Law).

([144]) D.w.z. in geval van opzettelijke inmenging in iemands privézaken of -belangen, op een manier die voor een redelijk persoon zeer beledigend zou zijn (Restatement (2nd) of Torts, § 652(b)).

([145]) Deze onrechtmatige daad wordt gewoonlijk toegepast in geval van toe-eigening en gebruik van iemands naam of gelijkenis om reclame te maken voor een bedrijf of product, of voor een soortgelijk commercieel doel (zie Restatement (2nd) of Torts, § 652C).

([146]) D.w.z. wanneer informatie betreffende het privéleven van een natuurlijk persoon openbaar wordt gemaakt, wanneer dit voor een redelijk persoon zeer beledigend is en de informatie niet van legitiem belang is voor het publiek (Restatement (2nd) of Torts, § 652D).

([147]) Dit is ook relevant in het licht van bijlage I, hoofdstuk I, punt 5. Volgens dit hoofdstuk en gelijklopend met de AVG kunnen er beperkingen gelden op de naleving van de vereisten voor de bescherming van gegevens en op de rechten die deel uitmaken van de privacybeginselen. Die beperkingen zijn echter niet absoluut, maar kunnen alleen in bepaalde omstandigheden worden ingeroepen, bijvoorbeeld voor zover dat nodig is om een gerechtelijk bevel na te leven of te voldoen aan eisen van openbaar belang, rechtshandhaving of nationale veiligheid. Voor alle duidelijkheid: dit hoofdstuk verwijst in dit verband ook naar de in EO 14086 uiteengezette voorwaarden die onder andere zijn beoordeeld in de overwegingen 127-141.

([148]) Zie Schrems II, punten 174–175, en de aangehaalde rechtspraak. Zie ook, wat de toegang van overheidsinstanties van de lidstaten betreft, het arrest van het Hof, Privacy International, zaak C-623/17, ECLI:EU:C:2020:790, punt 65; en het arrest van het Hof, La Quadrature du Net e.a., gevoegde zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, punt 175.

([149]) Zie Schrems II, punten 176 en 181, en de aangehaalde rechtspraak. Zie ook, wat de toegang van overheidsinstanties van de lidstaten betreft, Privacy International, punt 68, en La Quadrature du Net e.a., punt 132.

afdwingbaar zijn door natuurlijke personen ([150]). Betrokkenen moeten met name de mogelijkheid hebben een rechtsvordering in te stellen bij een onafhankelijke en onpartijdige rechterlijke instantie om inzage te krijgen in hun persoonsgegevens of om deze gegevens te laten corrigeren of wissen ([151]).

3.1 De toegang van en het gebruik door de Amerikaanse overheidsdiensten met het oog op rechtshandhaving

(90) Wat betreft inmenging in persoonsgegevens die in het kader van het EU-VS-DPF worden doorgegeven voor rechtshandhavingsdoeleinden, legt het recht van de Verenigde Staten een aantal beperkingen op aan de toegang tot en het gebruik van persoonsgegevens, en voorziet het in toezichts- en verhaalmechanismen die in overeenstemming zijn met de in overweging 89 van dit besluit bedoelde vereisten. De voorwaarden waaronder deze toegang kan plaatsvinden en de waarborgen die van toepassing zijn op het gebruik van die bevoegdheden worden in de volgende punten in detail beoordeeld. In dit verband heeft de Amerikaanse overheid (via het ministerie van Justitie) ook garanties gegeven over de toepasselijke beperkingen en waarborgen (bijlage VI bij dit besluit).

3.1.1 *Rechtsgrondslagen, beperkingen en waarborgen*

3.1.1.1 *Beperkingen en waarborgen met betrekking tot het verzamelen van persoonsgegevens voor rechtshandhavingsdoeleinden*

(91) Door gecertificeerde Amerikaanse organisaties verwerkte persoonsgegevens die op basis van het EU-VS-DPF vanuit de Unie zouden worden doorgegeven, kunnen door Amerikaanse federale aanklagers en federale opsporingsambtenaren volgens verschillende procedures worden geraadpleegd voor rechtshandhavingsdoeleinden, zoals in de overwegingen 92 tot en met 99 nader wordt toegelicht. Deze procedures zijn op dezelfde wijze van toepassing wanneer informatie wordt verkregen van een Amerikaanse organisatie, ongeacht de nationaliteit of woonplaats van de betrokkenen ([152]).

(92) Ten eerste kan een rechter op verzoek van een federale wetshandhavingsfunctionaris of een advocaat van de overheid een bevel tot huiszoeking of inbeslagneming (met inbegrip van elektronisch opgeslagen informatie) uitvaardigen ([153]). Een dergelijk bevel kan alleen worden uitgevaardigd als er een "redelijk vermoeden" ([154]) bestaat dat "in beslag te nemen voorwerpen" (bewijsmateriaal van een misdrijf, illegaal in bezit gehouden voorwerpen, of voorwerpen die zijn ontworpen of bestemd voor gebruik of zijn gebruikt bij het plegen van een misdrijf) waarschijnlijk zullen worden gevonden op de in het bevel aangegeven plaats. Het bevel moet de in beslag te nemen goederen of voorwerpen identificeren en de rechter aanwijzen bij wie het bevel moet worden teruggezonden. Een

([150]) Zie Schrems II, punten 181–182.

([151]) Zie Schrems I, punt 95 en Schrems II, punt 194. In dat verband heeft het Hof met name benadrukt dat artikel 47 van het Handvest van de grondrechten (dat het recht op een doeltreffende voorziening in rechte bij een onafhankelijk en onpartijdig gerecht waarborgt), deel uitmaakt van "het binnen de Unie vereiste beschermingsniveau en [dat] de Commissie de naleving [ervan] moet vaststellen alvorens een adequaatheidsbesluit op grond van artikel 45, lid 1, AVG vast te stellen" (Schrems II, punt 186).

([152]) Zie bijlage VI. Zie bijvoorbeeld, met betrekking tot de Wiretap Act, de Stored Communications Act en de Pen Register Act (meer in detail genoemd in de overwegingen 95 tot en met 98), Suzlon Energy Ltd/Microsoft Corp, 671 F.3d 726, 729 (9th Cir. 2011).

([153]) Federal Rules of Criminal Procedure, 41. In een arrest uit 2018 heeft het Hooggerechtshof bevestigd dat rechtshandhavingsinstanties ook over een huiszoekingsbevel of een uitzonderlijke toelating tot huiszoeking zonder rechterlijk bevel moeten beschikken om toegang te krijgen tot historische locatiegegevens van mobiele telefoons, die een uitgebreid overzicht geven van de bewegingen van een gebruiker en dat de gebruiker een redelijke verwachting van privacy mag hebben met betrekking tot dergelijke informatie (Timothy Ivory Carpenter/United States of America, nr. 16-402, 585 U.S. (2018)). Bijgevolg kunnen dergelijke gegevens over het algemeen niet van een telecommunicatiebedrijf worden verkregen op basis van een rechterlijk bevel op basis van redelijke gronden om aan te nemen dat de informatie relevant en materieel is voor een lopend strafrechtelijk onderzoek, maar moet bij gebruik van een bevelschrift het bestaan van een redelijk vermoeden worden aangetoond.

([154]) Volgens het Hooggerechtshof is "redelijk vermoeden" een praktische, niet-technische norm die een beroep doet op de feitelijke en praktische overwegingen van het dagelijks leven op grond waarvan redelijke en voorzichtige mensen handelen (Illinois/Gates, 462 U. S. 213, 232 (1983)). Wat huiszoekingsbevelen betreft, is er sprake van redelijk vermoeden wanneer er een redelijke waarschijnlijkheid is dat een huiszoeking zal leiden tot de ontdekking van bewijsmateriaal voor een misdrijf (Illinois/Gates).

persoon die wordt onderworpen aan een zoeking of wiens eigendom wordt doorzocht, kan verzoeken om vernietiging van bewijs dat is verkregen of afgeleid van een onrechtmatige doorzoeking indien dat bewijs tijdens een strafproces tegen die persoon wordt ingebracht ([155]). Wanneer een houder van gegevens (bv. een onderneming) op grond van een bevel verplicht is gegevens openbaar te maken, kan hij de verplichting tot openbaarmaking met name aanvechten als een te zware last ([156]).

(93) Ten tweede kan een dwangbevel worden uitgevaardigd door een kamer van inbeschuldigingstelling (*grand jury*) (een door een rechter of magistraat ingestelde onderzoekstak van de rechtbank) in het kader van onderzoeken naar bepaalde ernstige misdrijven ([157]), gewoonlijk op verzoek van een federale openbaar aanklager, om iemand te verplichten bedrijfsdocumenten, elektronisch opgeslagen informatie of andere tastbare zaken over te leggen of beschikbaar te stellen. Bovendien is het op grond van verschillende wetten toegestaan om administratieve dwangbevelen te gebruiken om bedrijfsgegevens, elektronisch opgeslagen informatie of andere tastbare zaken over te leggen of ter beschikking te stellen in onderzoeken betreffende gezondheidszorgfraude, kindermisbruik, bescherming van de geheime dienst, zaken over gecontroleerde stoffen en onderzoeken van de inspecteur-generaal (*Inspector General*) waarbij overheidsinstanties betrokken zijn ([158]). In beide gevallen moet de informatie relevant zijn voor het onderzoek en mag het dwangbevel niet onredelijk zijn, d.w.z. te ruim, te zwaar of belastend (en kan het door de ontvanger van het dwangbevel op die gronden worden aangevochten) ([159]).

(94) Voor administratieve dwangbevelen die worden uitgevaardigd voor de toegang van civiele of regelgevende instanties (in het openbaar belang) tot gegevens die in het bezit zijn van ondernemingen in de Verenigde Staten gelden zeer vergelijkbare voorwaarden. De bevoegdheid van instanties met civiele en regelgevende verantwoordelijkheden om dergelijke administratieve dwangbevelen uit te vaardigen, moet bij wet zijn vastgelegd. Het gebruik van een administratief dwangbevel wordt onderworpen aan een "redelijkheidstest", waarbij wordt vereist dat het onderzoek uit hoofde van een gerechtvaardigd doel wordt verricht, dat de in het kader van het dwangbevel gevraagde informatie relevant is voor dat doel, dat de instantie nog niet beschikt over de informatie die zij met het dwangbevel opvraagt, en dat voor de uitvaardiging van het dwangbevel de nodige administratieve stappen werden gevolgd ([160]). Jurisprudentie van het Hooggerechtshof heeft ook verduidelijkt dat het algemeen belang bij de gevraagde informatie even zwaar moet wegen als de privacybelangen van personen en organisaties ([161]). Hoewel het gebruik van een administratief dwangbevel niet vooraf door een rechter moet worden goedgekeurd, wordt het wel aan rechterlijke toetsing onderworpen als de ontvanger het dwangbevel op de hierboven vermelde gronden aanvecht, of als de instantie die het dwangbevel heeft uitgevaardigd, het dwangbevel wil gebruiken in de rechtbank ([162]). Naast deze algemene overkoepelende beperkingen, kunnen specifieke (strengere) eisen voortvloeien uit afzonderlijke wetten ([163]).

([155]) Mapp/Ohio, 367 U.S. 643 (1961).

([156]) Zie In re Application of United States, 610 F.2d 1148, 1157 (3d Cir. 1979) (waarin wordt gesteld dat eerlijke rechtsgang vereist dat een hoorzitting wordt gehouden over de kwestie van de last alvorens een telefoonmaatschappij te verplichten bijstand te verlenen bij een huiszoekingsbevel) en In re Application of United States, 616 F.2d 1122 (9th Cir. 1980.

([157]) Het vijfde amendement van de Amerikaanse grondwet vereist een aanklacht door een kamer van inbeschuldigingstelling (grand jury) voor elke halsmisdaad of anderszins schandelijke misdaad. De kamer van inbeschuldigingstelling bestaat uit 16 tot 23 leden, en bepaalt of er een redelijk vermoeden is om aan te nemen dat er een misdrijf is gepleegd. Om tot deze conclusie te komen, hebben de kamers van inbeschuldigingstelling onderzoeksbevoegdheden die hen in staat stellen dwangbevelen uit te vaardigen.

([158]) Zie bijlage VI.

([159]) Federal Rules of Criminal Procedure, 17.

([160]) Verenigde Staten/Powell, 379 U.S. 48 (1964).

([161]) Oklahoma Press Publishing Co./Walling, 327 U.S. 186 (1946).

([162]) Het Hooggerechtshof heeft verduidelijkt dat een rechter, indien een administratief dwangbevel wordt aangevochten, moet nagaan of (1) het onderzoek een rechtmatig toegestaan doeleinde dient, (2) de instantie die het dwangbevel in kwestie heeft uitgevaardigd onder de bevoegdheid van het Congres valt en (3) de gezochte documenten relevant zijn voor het onderzoek. Het Hooggerechtshof heeft ook opgemerkt dat een aanvraag van een administratief dwangbevel redelijk moet zijn, d.w.z. dat de specificatie van de te verstrekken documenten adequaat, maar niet buitensporig moet zijn voor de doeleinden van het desbetreffende onderzoek, en dat bijzonderheden moeten worden gegeven in de beschrijving van de te doorzoeken plaats en de betrokken personen of de in beslag te nemen goederen.

([163]) De Right to Financial Privacy Act, bijvoorbeeld, geeft een overheidsinstantie op grond van een administratief dwangbevel uitsluitend de bevoegdheid om financiële gegevens van een financiële instelling te verkrijgen op voorwaarde dat (1) er reden is om aan te nemen dat de gezochte gegevens relevant zijn voor een legitiem onderzoek in het kader van de rechtshandhaving en (2) de klant een kopie van het dwangbevel of de dagvaarding heeft gekregen, samen met een kennisgeving waarin de aard van het onderzoek in redelijk nadere bijzonderheden wordt beschreven (12 U.S.C. §3405). Een ander voorbeeld is de Fair Credit Reporting Act. Deze verbiedt agentschappen die de kredietwaardigheid van consumenten onderzoeken om consumentenkredietverslagen bekend te maken als reactie op aanvragen van een administratief dwangbevel (deze wet staat hen uitsluitend toe te reageren op dwangbevelen van de kamer van inbeschuldigingstelling of van rechterlijke instanties, 15 U.S.C. §1681 e.v.). Wat betreft de toegang tot communicatiegegevens gelden de specifieke voorschriften van de Stored Communications Act, ook met betrekking tot de mogelijkheid om administratieve dwangbevelen te gebruiken (zie de overwegingen 96 tot en met 97 voor een uitvoerig overzicht).

(95) Ten derde zijn er verschillende rechtsgrondslagen op basis waarvan rechtshandhavingsinstanties toegang kunnen krijgen tot communicatiegegevens. Een rechter kan een bevel afgeven waarbij toestemming wordt verleend voor het verzamelen van realtime, niet-inhoudgerelateerde kies-, routerings-, adresserings- en SIGINT-informatie over een telefoonnummer of e-mail (door middel van een *pen register* of een *trap and trace device* (trackers van berichtenverkeer)), indien hij vaststelt dat de autoriteit heeft verklaard dat de waarschijnlijk te verkrijgen informatie relevant is voor een lopend strafrechtelijk onderzoek ([164]). Het bevel moet onder meer de identiteit, indien bekend, van de verdachte vermelden; de kenmerken van de communicatie waarop het van toepassing is en een vermelding van het strafbare feit waarop de te verzamelen informatie betrekking heeft. Het gebruik van een *pen register* of een *trap and trace device* (trackers van berichtenverkeer) kan worden toegestaan voor een periode van maximaal zestig dagen, die alleen door een nieuw rechterlijk bevel kan worden verlengd.

(96) Bovendien kan op grond van de Stored Communications Act ([165])voor rechtshandhavingsdoeleinden toegang worden verkregen tot abonnee-informatie, verkeersgegevens en opgeslagen communicatie-inhoud waarover internetproviders, telefoonmaatschappijen en andere externe dienstverleners beschikken. Voor het verkrijgen van de opgeslagen inhoud van elektronische communicatie moeten rechtshandhavingsinstanties in principe een huiszoekingsbevel verkrijgen van een rechter op basis van een redelijk vermoeden om aan te nemen dat de desbetreffende account bewijs bevat van een misdrijf ([166]). Voor het verkrijgen van informatie over abonnees, IP-adressen en bijbehorende tijdcodes, evenals van factuurinformatie kunnen rechtshandhavingsinstanties een dwangbevel gebruiken. Voor de meeste andere opgeslagen, niet-inhoudgerelateerde informatie, zoals e-mailheaders zonder onderwerpregel, moeten rechtshandhavingsinstanties een gerechtelijk bevel verkrijgen, dat zal worden uitgevaardigd als de rechter ervan overtuigd is dat er redelijke gronden zijn om aan te nemen dat de gevraagde informatie relevant is en van materieel belang voor een lopend strafrechtelijk onderzoek.

(97) Providers die op grond van de Stored Communications Act verzoeken ontvangen, kunnen een klant of abonnee wiens informatie wordt opgevraagd, daarvan vrijwillig in kennis stellen, behalve wanneer de betrokken rechtshandhavingsinstantie een beschermingsbevel verkrijgt dat een dergelijke kennisgeving verbiedt ([167]). Een dergelijk beschermingsbevel is een rechterlijk bevel op grond waarvan een provider van elektronische communicatiediensten of computerdiensten op afstand, tot wie een bevel, dagvaarding of rechterlijk bevel is gericht, geen andere personen in kennis mag stellen van het bestaan van het bevel, de dagvaarding of het rechterlijk bevel, zolang de rechter dat nodig acht. Beschermingsbevelen worden gegeven als een rechter oordeelt dat er reden is om aan te nemen dat kennisgeving een onderzoek ernstig in gevaar zou brengen of een proces onnodig zou vertragen, bijvoorbeeld omdat dit het leven of de fysieke veiligheid van een persoon in gevaar zou brengen, omdat hij zou vluchten voor vervolging, omdat potentiële getuigen zouden worden geïntimideerd enz. Volgens een memorandum van de viceminister van Justitie (*Deputy Attorney General)* (dat bindend is voor alle advocaten en functionarissen van het ministerie van Justitie) moeten openbaar aanklagers een gedetailleerde beslissing nemen over de noodzaak van een beschermingsbevel en voor de rechter motiveren hoe in de specifieke zaak aan de wettelijke criteria voor het verkrijgen van een beschermingsbevel is voldaan ([168]). Het memorandum bepaalt ook dat verzoeken om een beschermingsbevel in het algemeen niet tot doel mogen hebben de kennisgeving langer dan een jaar uit te stellen. Wanneer in uitzonderlijke omstandigheden bevelen van langere duur nodig zijn, kunnen deze alleen worden gevraagd met de schriftelijke instemming van een door de *U.S. Attorney* (Amerikaanse federale hoofdaanklager) of de bevoegde adjunct-minister van Justitie (*Assistant Attorney General*) aangewezen toezichthouder. Bovendien moet een openbaar aanklager bij de afsluiting van een onderzoek onmiddellijk nagaan of er een grond is om nog lopende beschermingsbevelen te handhaven en, indien dat niet het geval is, het beschermingsbevel beëindigen en ervoor zorgen dat de dienstverlener daarvan in kennis wordt gesteld ([169]).

([164]) 18 U.S.C. § 3123.

([165]) 18 U.S.C. §§ 2701-2713.

([166]) 18 U.S.C. §§ 2701(a)-(b)(1)(A). Indien de betrokken abonnee of klant in kennis wordt gesteld (hetzij vooraf, hetzij onder bepaalde omstandigheden via een uitgestelde kennisgeving), kan de inhoudgerelateerde informatie die langer dan 180 dagen is opgeslagen, ook worden verkregen op basis van een administratief dwangbevel of een dwangbevel van een kamer van inbeschuldigingstelling (18 U.S.C § 2701(b)(1)(B)) of een gerechtelijk bevel (indien er redelijke gronden zijn om aan te nemen dat de informatie relevant is en van materieel belang voor een lopend strafrechtelijk onderzoek (18 U.S.C § 2701(d)). Volgens een uitspraak van een federaal hof van beroep krijgen overheidsonderzoekers echter doorgaans een huiszoekingsbevel van een rechter om de inhoud van privécommunicatie of opgeslagen gegevens van een commerciële provider van communicatiediensten te verzamelen. United States/Warshak, 631 F.3d 266 (6th Cir. 2010).

([167]) 18 U.S.C. § 2705(b).

([168]) Memorandum van viceminister van Justitie Rod Rosenstein van 19 oktober 2017 over een restrictiever beleid inzake verzoeken om beschermingsbevelen (of niet-openbaarmakingsbevelen), beschikbaar op https://www.justice.gov/criminal-ccips/page/file/1005791/download

([169]) Memorandum van viceminister van Justitie Lisa Moncao van 27 mei 2022 over een aanvullend beleid inzake verzoeken om beschermingsbevelen overeenkomstig 18 U.S.C. § 2705(b).

(98) Rechtshandhavingsinstanties kunnen ook in real time kabel-, mondeling of elektronisch communicatieverkeer aftappen op basis van een gerechtelijk bevel waarin een rechter onder meer vaststelt dat er een redelijk vermoeden is om te geloven dat het afluisteren of de elektronische onderschepping bewijs zal opleveren van een federaal misdrijf of de locatie van een voortvluchtige die vervolging ontvlucht ([170]).

(99) Verdere bescherming wordt geboden door verschillende beleidslijnen en richtsnoeren van het ministerie van Justitie, waaronder de richtsnoeren van de minister van Justitie in verband met binnenlandse FBI-operaties (AGG-DOM), die onder meer voorschrijven dat het Federal Bureau of Investigation (de FBI) de minst ingrijpende onderzoeksmethoden als haalbaar gebruikt, rekening houdend met de gevolgen voor de privacy en de burgerlijke vrijheden ([171]).

(100) Volgens de verklaringen van de Amerikaanse overheid geldt dezelfde of grotere bescherming zoals hierboven beschreven voor rechtshandhavingsonderzoeken op het niveau van de staten (met betrekking tot onderzoek dat krachtens de wetgeving van de staten wordt uitgevoerd) ([172]). De bovenvermelde bescherming tegen onredelijke huiszoekingen en inbeslagnemingen wordt met name bevestigd door grondwettelijke bepalingen, evenals wetten en rechtspraak op het niveau van de staten, doordat deze de uitvaardiging van een huiszoekingsbevel vereisen ([173]). Net zoals bij de bescherming die op federaal niveau wordt geboden, kunnen huiszoekingsbevelen uitsluitend worden uitgevaardigd indien een redelijk vermoeden wordt aangetoond en moeten in die bevelen de te doorzoeken plaats en de betrokken personen of de in beslag te nemen goederen worden beschreven ([174]).

([170]) 18 U.S.C. §§ 2510-2522.

([171]) Richtsnoeren van de minister van Justitie in verband met binnenlandse operaties van het Federal Bureau of Investigation (FBI) (september 2008), beschikbaar op http://www.justice.gov/archive/opa/docs/guidelines.pdf. Aanvullende voorschriften en beleidsmaatregelen waarin beperkingen aan onderzoeksactiviteiten van federale aanklagers zijn vastgesteld, zijn opgenomen in het United States Attorneys' Manual, beschikbaar op http://www.justice.gov/usam/united-states-attorneys-manual Om van deze richtsnoeren af te wijken, moet vooraf toestemming worden verkregen van de directeur, de vicedirecteur of de door de directeur aangewezen uitvoerend adjunct-directeur van de FBI, tenzij deze toestemming niet kan worden verkregen wegens de onmiddellijke of ernstige bedreiging van de veiligheid van personen of goederen of van de nationale veiligheid (in welk geval de directeur of een andere bevoegde persoon zo spoedig mogelijk in kennis moet worden gesteld). Wanneer de richtsnoeren niet worden gevolgd, moet de FBI het ministerie van Justitie daarvan in kennis stellen, dat op zijn beurt de minister van Justitie en de viceminister van Justitie informeert.

([172]) Bijlage VI, voetnoot 2. Zie bv. ook Arnold/City of Cleveland, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) ("In the areas of individual rights and civil liberties, the United States Constitution, where applicable to the states, provides a floor below which state court decisions may not fall"— Wat de individuele rechten en burgerlijke vrijheden betreft, zorgt de grondwet van de Verenigde Staten, wanneer deze op de staten van toepassing is, voor een ondergrens die door de beslissingen van de staatsrechtbank niet mag worden overschreden); Cooper/California, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) ("Our holding, of course, does not affect the State's power to impose higher standards on searches and seizures than required by the Federal Constitution if it chooses to do so." — Ons standpunt heeft uiteraard geen gevolgen voor de bevoegdheid van de staat om aan huiszoekingen en inbeslagnemingen hogere normen op te leggen dan die welke door de federale grondwet worden vereist, als de staat dit zou willen doen); Petersen/City of Mesa, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) ("Although the Arizona Constitution may impose stricter standards on searches and seizures than does the federal constitution, Arizona courts cannot provide less protection than does the Fourth Amendment" — Hoewel de grondwet van Arizona aan huiszoekingen en inbeslagnemingen strengere normen kan opleggen dan de federale grondwet, kunnen de rechtbanken van Arizona niet minder bescherming geven dan die geboden door het Vierde amendement).

([173]) De meeste staten hebben de bescherming van het Vierde amendement overgenomen in hun eigen grondwet. Zie Alabama Const. art. I, § 5); Alaska Const. art. I, § 14; 1; Arkansas Const. art. II, § 15; California Const. art. I, § 13; Colorado Const. art. II, § 7; Conneticut Const. art. I, § 7; Delaware Const. art. I, § 6; Florida. Const. art. I, § 12; Georgia Const. art. I, § I, para. XIII; Hawai Const. art. I, § 7; Idaho Const. art. I, § 17; Illinois Const. art. I, § 6; Indiana Const. art. I, § 11; Iowa Const. art. I, § 8; Kansas Const. Bill of Rights, § 15; Kentucky Const. § 10; Louisiana Const. art. I, § 5; Maine Const. art. I, § 5; Massachusets Const. Decl. of Rights art. 14; Michigan Const. art. I, § 11; Minnesota Const. art. I, § 10; Mississippi Const. art. III, § 23; Missouri Const. art. I, § 15; Montana Const. art. II, § 11; Nebraska Const. art. I, § 7; Nevada Const. art. I, § 18; New Hampshire Const. pt. 1, art. 19; N.J. Const. art. II, § 7; New Mexico Const. art. II, § 10; New York Const. art. I, § 12; North Dakota Const. art. I, § 8; Ohio Const. art. I, § 14; Oklahoma Const. art. II, § 30; Oregon Const. art. I, § 9; Pennsylvania Const. art. I, § 8; Rhode Island Const. art. I, § 6; South Carolina Const. art. I, § 10; South Dakota Const. art. VI, § 11; Tennessee Const. art. I, § 7; Texas Const. art. I, § 9; Utah Const. art. I, § 14; Vermont Const. ch. I, art. 11; West Virginia Const. art. III, § 6; Wisconsin Const. art. I, § 11; Wyoming Const. art. I, § 4. Andere staten (bv. Maryland, North Carolina en Virginia) hebben in hun grondwet specifieke formuleringen opgenomen betreffende bevelschriften, die volgens juridische interpretatie een even goede of betere bescherming bieden dan het Vierde amendement (zie Maryland. Decl. of Rts. art. 26; North Carolina Const. art. I, § 20; Virginia Const. art. I, § 10, en desbetreffende rechtspraak, bv. Hamel/State, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008; State/Johnson, 861 S.E.2d 474, 483 (N.C. 2021) en Lowe/ Commonwealth, 337 S.E.2d 273, 274 (Va. 1985)). Tot slot hebben Arizona en Washington grondwettelijke bepalingen die de privacy meer in het algemeen beschermen (Arizona Const. art. 2, § 8; Washington Const. art. I, § 7), en die door rechtbanken zijn geïnterpreteerd als een sterkere bescherming dan die welke wordt geboden door het Vierde amendement (zie bv. State/Bolt, 689 P.2d 519, 523 (Ariz. 1984), State/Ault, 759 P.2d 1320, 1324 (Ariz. 1988), State/Myrick, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984) , State/Young, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)).

([174]) Zie bv. California Penal Code § 1524,3(b); Rule 3.6-3.13 Alabama Rules of Criminal Procedure; Section 10.79.035; Revised Code of Washington; Section 19.2-59 of Chapter 5, Title 19.2 Criminal Procedure, Code of Virginia.

3.1.1.2 *Verder gebruik van de verzamelde informatie*

(101) Wat het verdere gebruik van door federale rechtshandhavingsinstanties verzamelde gegevens betreft, leggen verschillende wetten, richtsnoeren en normen specifieke waarborgen op. Met uitzondering van de specifieke instrumenten die van toepassing zijn op de activiteiten van de FBI (AGG-DOM en de FBI Domestic Investigations and Operations Guide), zijn de in dit hoofdstuk beschreven voorschriften in het algemeen van toepassing op het verdere gebruik van gegevens door een federale instantie, met inbegrip van gegevens die worden geraadpleegd voor civiele en regelgevende doeleinden. Dit omvat de voorschriften die voortvloeien uit memoranda/regelgeving van het Office of Management and Budget, de Federal Information Security Management Modernization Act, de E-Government Act en de Federal Records Act.

(102) In overeenstemming met de bevoegdheid die wordt verleend door de Clinger-Cohen Act (P.L. 104-106, Division E) en de Computer Security Act van 1987 (P.L. 100-235), heeft het *Office of Management and Budget* (bureau voor Beheer en Begroting, hierna "OMB") circulaire nr. A-130 uitgegeven om algemene bindende richtsnoeren vast te stellen die van toepassing zijn op alle federale instanties (met inbegrip van wetshandhavingsinstanties) wanneer zij persoonsgegevens verwerken ([175]). De circulaire schrijft met name voor dat alle federale instanties het creëren, verzamelen, gebruiken, verwerken, opslaan, bijhouden, verspreiden en openbaar maken van persoonlijk identificeerbare informatie moeten beperken tot hetgeen wettelijk is toegestaan, relevant is en redelijkerwijs noodzakelijk wordt geacht voor de goede uitvoering van de toegestane taken van de instantie ([176]). Bovendien moeten federale instanties, voor zover dit redelijkerwijs mogelijk is, ervoor zorgen dat persoonlijk identificeerbare informatie nauwkeurig, relevant, tijdig en volledig is en beperkt wordt tot het minimum dat nodig is voor de goede uitvoering van de taken van een instantie. Meer in het algemeen moeten federale instanties een uitgebreid privacyprogramma opstellen om de naleving van de toepasselijke privacyvoorschriften te waarborgen, een privacybeleid te ontwikkelen en te evalueren en privacyrisico's te beheren; procedures handhaven om incidenten in verband met de naleving van de privacy op te sporen, te documenteren en te rapporteren; bewustmakings- en opleidingsprogramma's inzake privacy ontwikkelen voor werknemers en contractanten; en beleid en procedures in te voeren om ervoor te zorgen dat het personeel verantwoordelijk wordt gehouden voor de naleving van de privacyvoorschriften en het beleid ([177]).

(103) Bovendien vereist de E-Government Act ([178]) dat alle federale instanties (met inbegrip van rechtshandhavingsinstanties) informatiebeveiliging instellen die in verhouding staat tot het risico en de omvang van de schade die zou voortvloeien uit ongeoorloofde toegang, gebruik, openbaarmaking, verstoring, wijziging of vernietiging; een *Chief Information Officer* hebben die toeziet op de naleving van de informatiebeveiligingsvoorschriften en jaarlijks een onafhankelijke evaluatie (bijvoorbeeld door een inspecteur-generaal, zie overweging 109) van hun informatiebeveiligingsprogramma en -praktijken uitvoeren ([179]). Evenzo vereisen de Federal Records Act (de federale archiefwet, FRA) ([180]) en de aanvullende voorschriften ([181]) dat informatie in het bezit van federale instanties onderworpen wordt aan waarborgen die de fysieke integriteit van de informatie waarborgen en deze beschermen tegen toegang door onbevoegden.

(104) Op grond van een federale wettelijke bevoegdheid, waaronder de Federal Information Security Modernisation Act van 2014, hebben het OMB en het National Institute of Standards and Technology (NIST) normen ontwikkeld die bindend zijn voor federale instanties (waaronder rechthandhavingsinstanties) en die verder specificeren welke minimumvereisten op het gebied van informatiebeveiliging moeten worden ingevoerd, waaronder toegangscontroles, zorgen voor bewustmaking en opleiding, noodplannen, reactie op incidenten, audit- en verantwoordingsinstrumenten, zorgen voor systeem- en informatie-integriteit, uitvoeren van privacy- en beveiligingsrisicobeoordelingen enz. ([182]). Bovendien moeten alle federale instanties (inclusief rechtshandhavingsin-

([175]) D.w.z. informatie die kan worden gebruikt om de identiteit van een persoon te onderscheiden of op te sporen, hetzij alleen, hetzij in combinatie met andere informatie die aan een specifieke persoon is gekoppeld of kan worden gekoppeld, zie circulaire nr. A-130 van het OMB, blz. 33 (definitie van "persoonlijk identificeerbare informatie").

([176]) Circulaire nr. A-130 van het OMB, "Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information" [Informatie beheren als strategische hulpbron, aanhangsel II, Verantwoordelijkheden voor het beheer van persoonlijk identificeerbare informatie], 81 Fed. Reg. 49.689 (28 juli 2016), blz. 17.

([177]) Aanhangsel II, § 5, (a)-(h).

([178]) 44 U.S.C. Chapter 36.

([179]) 44 U.S.C. §§ 3544-3545.

([180]) FAC, 44 U.S.C. § 3105.

([181]) 36 C.F.R. §§ 1228,150, e.v., 1228,228, en aanhangsel A.

([182]) Zie bijvoorbeeld circulaire nr. A-130 van het OMB; NIST SP 800-53, Rev. 5, "Security and Privacy Controls for Information Systems and Organizations" [Beveiligings- en privacycontroles voor informatiesystemen en -organisaties] (10 december 2020); en de "Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems" [Federale informatieverwerkingsnormen 200: minimumbeveiligingsvereisten voor federale informatie en informatiesystemen] van het NIST.

stanties), overeenkomstig de richtsnoeren van het OMB, een plan voor de aanpak van datalekken bijhouden en uitvoeren, ook wat betreft het reageren op dergelijke inbreuken en het beoordelen van de risico's op schade ([183]).

(105) Wat de bewaring van gegevens betreft, verplicht de federale archiefwet ([184]) de federale instanties van de VS (met inbegrip van de rechtshandhavingsinstanties) bewaartermijnen voor hun gegevens vast te stellen (waarna deze moeten worden verwijderd), die moeten worden goedgekeurd door de *National Archives and Record Administration* ([185]). De duur van deze bewaartermijn wordt vastgesteld in het licht van verschillende factoren, zoals het soort onderzoek, de vraag of het bewijsmateriaal nog relevant is voor het onderzoek enz. Met betrekking tot de FBI bepalen de AGG-DOM dat de FBI over een dergelijk plan voor het bewaren van gegevens moet beschikken en een systeem moet onderhouden waarmee de status van en de grondslag voor onderzoeken snel kunnen worden teruggevonden.

(106) Ten slotte bevat circulaire nr. A-130 van het OMB ook bepaalde voorschriften voor de verspreiding van persoonsgegevens. In beginsel moet de verspreiding en openbaarmaking van persoonsgegevens worden beperkt tot wat wettelijk is toegestaan en tot wat relevant en redelijkerwijs noodzakelijk wordt geacht voor de correcte uitvoering van de taken van een instantie ([186]). Wanneer zij persoonlijk identificeerbare informatie delen met andere overheidsinstanties, moeten de Amerikaanse federale instanties, waar nodig, voorwaarden opleggen (waaronder de uitvoering van specifieke beveiligings- en privacycontroles) die de verwerking van de informatie regelen door middel van schriftelijke overeenkomsten (waaronder contracten, overeenkomsten inzake gegevensgebruik, overeenkomsten inzake informatie-uitwisseling en memoranda van overeenstemming) ([187]). Wat betreft de gronden waarop informatie mag worden verspreid, bepalen de AGG-DOM en de FBI Domestic Investigations and Operations Guide ([188]) bijvoorbeeld dat de FBI informatie mag verspreiden wanneer hij daar wettelijk toe verplicht is (bv. in het kader van een internationale overeenkomst) dan wel in bepaalde omstandigheden, bv. aan andere Amerikaanse instanties indien openbaarmaking verenigbaar is met het doeleinde waarvoor de informatie werd verzameld en indien dit verband houdt met zijn verantwoordelijkheden; aan commissies van het Congres; aan buitenlandse instanties indien de informatie verband houdt met hun verantwoordelijkheden en de verspreiding ervan strookt met de belangen van de Verenigde Staten; de verspreiding is met name nodig om de veiligheid of de beveiliging van personen of goederen te beschermen, of om te beschermen tegen een misdrijf of een bedreiging van de nationale veiligheid en de openbaarmaking is verenigbaar met het doeleinde waarvoor de informatie werd verzameld ([189]).

3.1.2 ***Toezicht***

(107) De activiteiten van de federale rechtshandhavingsinstanties staan onder toezicht van verschillende instanties ([190]). Zoals toegelicht in de overwegingen 92 - 99 omvat dit meestal voorafgaand toezicht door de rechterlijke macht, die toestemming moet geven voor individuele maatregelen inzake verzameling voordat deze kunnen worden gebruikt. Daarnaast houden andere instanties toezicht op verschillende stadia in de activiteiten van de rechtshandhavingsinstanties, onder meer op de verzameling en verwerking van persoonsgegevens. Samen zorgen deze gerechtelijke en buitengerechtelijke instanties ervoor dat de rechtshandhavingsinstanties aan onafhankelijk toezicht worden onderworpen.

([183]) Memorandum 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" [Voorbereiding en reactie op een inbreuk op persoonlijk identificeerbare informatie], beschikbaar op https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf en circulaire nr. A-130 van het OMB. Bijvoorbeeld de procedures voor het reageren op datalekken van het ministerie van Justitie, zie https://www.justice.gov/file/4336/download

([184]) FRA, 44 U.S.C. §§ 3101 e.v.

([185]) De National Archives and Record Administration heeft de bevoegdheid om de praktijken van instanties op het gebied van archiefbeheer te beoordelen, en kan bepalen of verdere bewaring van bepaalde archiefstukken gerechtvaardigd is (44 U.S.C. § 2904, (c), § 2906).

([186]) Circulaire nr. A-130 van het OMB, sectie 5.f.1.(d).

([187]) Circulaire nr. A-130 van het OMB, aanhangsel I § 3, (d).

([188]) Zie ook FBI Domestic Investigations and Operations Guide (DIOG), sectie 14.

([189]) AGG-DOM, sectie VI, B en C; FBI Domestic Investigations and Operations Guide (DIOG), sectie 14.

([190]) De in dit hoofdstuk vermelde mechanismen gelden ook voor de verzameling en het gebruik van gegevens door federale instanties voor civiele en regelgevende doeleinden. Federale civiele en regelgevende instanties staan onder het toezicht van hun respectieve inspecteurs-generaal en van het Congres, onder meer het Government Accountability Office, de instantie van het Congres die audits en onderzoeken verricht. Tenzij de instantie beschikt over een eigen Privacy and Civil Liberties Officer (functionaris voor de bescherming van de privacy en de burgerlijke vrijheden) — een functie die normaliter bestaat binnen instanties zoals het ministerie van Justitie en het ministerie van Binnenlandse Veiligheid gezien hun verantwoordelijkheden op het gebied van rechtshandhaving en nationale veiligheid — behoren deze taken tot de opdracht van de Senior Agency Official for Privacy (SAOP, eerstaanwezend privacyfunctionaris) van de instantie. Alle federale instanties zijn wettelijk verplicht een SAOP aan te wijzen, die verantwoordelijk is voor de naleving van de privacywetgeving door de instantie en die toezicht houdt op aangelegenheden in verband daarmee. Zie bv. OMB M-16-24, "Role and Designation of Senior Agency Officials for Privacy" [Rol en aanwijzing van eerstaanwezend privacyfunctionarissen] (2016).

(108) Ten eerste bestaan er binnen verschillende diensten met verantwoordelijkheden op het vlak van rechtshandhaving functionarissen voor privacy en burgerlijke vrij*heden (Privacy and Civil Liberties Officers*) ([191]). Hoewel de specifieke bevoegdheden van deze functionarissen enigszins kunnen variëren afhankelijk van de rechtsgrondslag, omvatten ze doorgaans het toezicht op de procedures om ervoor te zorgen dat het/de respectieve ministerie/instantie op passende wijze rekening houdt met kwesties in verband met de privacy en de burgerlijke vrijheden, en passende procedures heeft ingevoerd voor de behandeling van klachten van natuurlijke personen die van mening zijn dat er inbreuk is gemaakt op hun privacy of burgerlijke vrijheden. De hoofden van elk ministerie of elke instantie moeten ervoor zorgen dat de functionarissen voor privacy en burgerlijke vrijheden beschikken over het materiaal en de middelen om hun mandaat te vervullen, toegang krijgen tot al het materiaal en personeel dat nodig is om hun taken uit te voeren, en worden geïnformeerd over en geraadpleegd over voorgestelde beleidswijzigingen ([192]). De functionarissen voor privacy en burgerlijke vrijheden brengen periodiek verslag uit aan het Congres, onder meer over het aantal en de aard van de klachten die het ministerie/de instantie heeft ontvangen en het gevolg dat aan die klachten is gegeven, de uitgevoerde controles en onderzoeken en de gevolgen van de door de functionaris verrichte activiteiten ([193]).

(109) Ten tweede houdt een onafhankelijke inspecteur-generaal (*Inspector General*) toezicht op de activiteiten van het ministerie van Justitie, met inbegrip van de FBI ([194]). Inspecteurs-generaal zijn wettelijk onafhankelijk ([195]) en verantwoordelijk voor het uitvoeren van onafhankelijke onderzoeken, audits en inspecties van de programma's en operaties van het ministerie. Zij hebben toegang tot alle gegevens, verslagen, audits, controles, documenten, papieren, aanbevelingen en ander relevant materiaal, zo nodig door een dwangbevel, en kunnen getuigenverklaringen afnemen ([196]). Hoewel inspecteurs-generaal niet-bindende aanbevelingen voor corrigerende maatregelen kunnen doen, worden hun verslagen, met inbegrip van de vervolgmaatregelen (of het ontbreken daarvan) ([197]) openbaar gemaakt en bovendien aan het Congres toegezonden, dat op basis daarvan zijn toezichtfunctie kan uitoefenen (zie overweging 111) ([198]).

([191]) Zie 42 U.S.C. § 2000ee-1. Hieronder vallen bijvoorbeeld het ministerie van Justitie, het ministerie van Binnenlandse Veiligheid en de FBI. Bij het ministerie van Binnenlandse Veiligheid is bovendien een functionaris voor privacy verantwoordelijk voor het behoud en de verbetering van de privacybescherming en de bevordering van transparantie binnen het ministerie (6 U.S.C. 142, sectie 222). Alle systemen, technologie, formulieren en programma's van het ministerie van Binnenlandse Veiligheid die persoonsgegevens verzamelen of gevolgen hebben voor de privacy, staan onder toezicht van de verantwoordelijke functionaris voor privacy, die toegang heeft tot alle gegevens, rapporten, audits, evaluaties, documenten, stukken, aanbevelingen en ander materiaal waarover het ministerie beschikt, zo nodig door middel van een dwangbevel. De functionaris voor privacy moet jaarlijks aan het Congres verslag uitbrengen over activiteiten van het ministerie die gevolgen hebben voor de privacy, met inbegrip van klachten over schendingen van de privacy.

([192]) 42 U.S.C. § 2000ee-1, (d).

([193]) Zie 42 U.S.C. § 2000ee-1, (f), (1)-(2). Uit het verslag van de verantwoordelijke functionaris voor privacy en burgerlijke vrijheden van het ministerie van Justitie en het bureau voor privacy en burgerlijke vrijheden over de periode oktober 2020-maart 2021 blijkt bijvoorbeeld dat er 389 privacybeoordelingen zijn uitgevoerd, onder meer van informatiesystemen en andere programma's (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

([194]) Evenzo is bij de Homeland Security Act van 2002 een ambt van inspecteur-generaal opgericht bij het ministerie van Binnenlandse Veiligheid.

([195]) Inspecteurs-generaal zijn vast benoemd en kunnen alleen worden ontslagen door de president, die het Congres schriftelijk op de hoogte moet brengen van de redenen voor een dergelijk ontslag.

([196]) Zie de Inspector General Act van 1978, § 6.

([197]) Zie in dit verband bijvoorbeeld het door het ambt van de inspecteur-generaal van het ministerie van Justitie opgestelde overzicht van de gedane aanbevelingen en de mate waarin deze zijn uitgevoerd door middel van vervolgmaatregelen van het ministerie en de instanties, https://oig.justice.gov/sites/default/files/reports/22-043.pdf

([198]) Zie de Inspector General Act van 1978, § 4(5) en § 5. Zo heeft het ambt van de inspecteur-generaal binnen het ministerie van Justitie onlangs zijn halfjaarlijks verslag aan het Congres gepubliceerd (1 oktober 2021 – 31 maart 2022, https://oig.justice.gov/node/23596), dat een overzicht geeft van zijn audits, evaluaties, inspecties, speciale beoordelingen en onderzoeken van programma's en operaties van het ministerie van Justitie. Deze activiteiten omvatten een onderzoek naar een voormalige contractant in verband met het onrechtmatig openbaar maken van elektronische surveillance (het afluisteren van een persoon) in een lopend onderzoek, dat leidde tot de veroordeling van de contractant. Het ambt van de inspecteur-generaal heeft ook een onderzoek uitgevoerd naar de informatiebeveiligingsprogramma's en -praktijken van de instanties van het ministerie van Justitie, waarbij de doeltreffendheid van het informatiebeveiligingsbeleid, de procedures en de praktijken van een representatieve subreeks van de systemen van de instanties werden getest.

(110) Ten derde staan ministeries met verantwoordelijkheden op het gebied van rechtshandhaving, voor zover zij terrorismebestrijdingsactiviteiten uitvoeren, onder toezicht van de *Privacy and Civil Liberties Oversight Board* (raad van toezicht op de privacy en de burgerlijke vrijheden, hierna "PCLOB"), een onafhankelijke instantie binnen de uitvoerende macht die bestaat uit een raad van vijf leden uit beide politieke partijen die door de president voor een vaste ambtstermijn van zes jaar zijn benoemd met goedkeuring van de Senaat ([199]). Volgens het oprichtingsstatuut is de PCLOB belast met verantwoordelijkheden op het gebied van terrorismebestrijding en de uitvoering daarvan, met het oog op de bescherming van de privacy en de burgerlijke vrijheden. Voor haar controle heeft deze instantie toegang tot alle relevante gegevens, verslagen, audits, controles, documenten, papieren en aanbevelingen van de diensten, inclusief gerubriceerde informatie, en kan zij gesprekken voeren en getuigen oproepen ([200]). Zij ontvangt de verslagen van de functionarissen voor de burgerlijke vrijheden en de privacy van verschillende federale ministeries/instanties ([201]), kan aanbevelingen doen aan de overheid en de wetshandhavingsinstanties en brengt regelmatig verslag uit aan de Committees (commissies) van het Congres en de president ([202]). Verslagen van de PCLOB, ook die aan het Congres, moeten zoveel mogelijk openbaar worden gemaakt ([203]).

(111) Ten slotte staan de activiteiten op het gebied van rechtshandhaving onder toezicht van specifieke *Committees* (commissies) in het Amerikaanse Congres (de commissies voor justitie van het Huis van Afgevaardigden en de Senaat). De commissies voor justitie oefenen hun toezichtfuncties op verschillende manieren uit, met name via hoorzittingen, onderzoeken, evaluaties en verslagen ([204]).

3.1.3 ***Verhaalmechanismemogelijkheden***

(112) Zoals aangegeven, moeten rechtshandhavingsinstanties in de meeste gevallen voorafgaande toestemming van de rechter verkrijgen om persoonsgegevens te verzamelen. Hoewel dit niet vereist is voor administratieve dwangbevelen, zijn deze beperkt tot specifieke situaties en zullen zij onderworpen zijn aan een onafhankelijke rechterlijke toetsing, althans wanneer de overheid om handhaving in rechte verzoekt. In het bijzonder kunnen de ontvangers van administratieve dwangbevelen deze bij de rechter aanvechten op grond van het feit dat ze onredelijk zijn, d.w.z. overdreven, onderdrukkend of belastend ([205]).

(113) Natuurlijke personen kunnen eerst en vooral bij de rechtshandhavingsinstanties vragen of klachten indienen betreffende de verwerking van hun persoonsgegevens. Dit omvat de mogelijkheid om te vragen of zij de persoonsgegevens mogen inzien en corrigeren ([206]). Wat activiteiten in verband met terrorismebestrijding betreft, kunnen natuurlijke personen ook een klacht indienen bij de functionarissen voor privacy en burgerlijke vrijheden (of andere privacyfunctionarissen) binnen de rechtshandhavingsinstanties ([207]).

(114) Bovendien voorziet de Amerikaanse wetgeving in een aantal gerechtelijke verhaalmechanismemogelijkheden voor natuurlijke personen tegen een overheidsinstantie of een van haar functionarissen, wanneer die instantie persoonsgegevens verwerkt ([208]). Die verhaalmechanismemogelijkheden, onder meer op grond van de APA, de Freedom of Information Act (FOIA) en de Electronic Communications Privacy Act (ECPA), staan open voor alle natuurlijke personen, ongeacht hun nationaliteit, onder de toepasselijke voorwaarden.

([199]) De leden van de PCLOB mogen uitsluitend worden geselecteerd op basis van hun beroepskwalificaties, prestaties, publieke status, deskundigheid op het gebied van burgerlijke vrijheden en privacy, en relevante ervaring, en ongeacht hun politieke kleur. In geen geval mogen meer dan drie leden van de raad tot dezelfde politieke partij behoren. Een in de PCLOB benoemde persoon mag tijdens zijn mandaat geen verkozen ambtenaar, functionaris of werknemer van de federale overheid zijn, anders dan in de hoedanigheid van lid van de PCLOB. Zie 42 U.S.C. § 2000ee, (h).

([200]) 42 U.S.C. § 2000ee, (g).

([201]) Zie 42 U.S.C. § 2000ee-1, (f), (1), (A), (iii). Hiertoe behoren ten minste het ministerie van Justitie, het ministerie van Defensie, het ministerie van Binnenlandse Veiligheid, plus eventuele andere ministeries, diensten of onderdelen van de uitvoerende macht waarvoor de PCLOB verslaggeving passend acht.

([202]) 42 U.S.C. § 2000ee, (e).

([203]) 42 U.S.C. § 2000ee, (f).

([204]) Zo organiseren de commissies thematische hoorzittingen (zie bv. een recente hoorzitting van het House Judiciary Committee over "digital dragnets", https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983), alsook regelmatige hoorzittingen over toezicht, bv. op de FBI en het ministerie van Justitie, zie https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 en https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899

([205]) Zie bijlage VI.

([206]) Circulaire nr. A-130 van het OMB, aanhangsel II, sectie 3, (a) en (f), waarin van federale instanties wordt verlangd dat zij zorgen voor passende inzage en correctie wanneer personen daarom vragen, en dat zij procedures vaststellen voor de ontvangst en behandeling van klachten en vragen in verband met privacy.

([207]) Zie 42 U.S.C. § 2000ee-1 met betrekking tot bijvoorbeeld het ministerie van Justitie en het ministerie van Binnenlandse Veiligheid. Zie ook Memorandum M-16-24 van het OMB, "Role and Designation of Senior Agency Officials for Privacy" [Rol en aanwijzing van eerstaanwezend privacyfunctionarissen].

([208]) De in dit hoofdstuk vermelde verhaalmechanismen gelden ook voor de verzameling en het gebruik van gegevens door federale instanties voor civiele en regelgevende doeleinden.

(115) De APA ([209]) voorziet algemeen in gerechtelijke verhaalmechanismemogelijkheden, op grond waarvan personen die onrechtmatig zijn behandeld door een overheid of die door een handeling van de overheid zijn benadeeld, zich tot het gerecht kunnen wenden ([210]). Dit omvat de mogelijkheid om van de rechterlijke instantie te vorderen dat zij vaststelt dat handelingen, vaststellingen en conclusies van de overheid willekeurig en onvoorspelbaar zijn, misbruik van discretionaire bevoegdheid inhouden of op andere wijze niet aan de wet voldoen, en dat zij die onrechtmatig en zonder gevolg verklaart ([211]).

(116) Meer specifiek wordt in titel II van de ECPA ([212]) een stelsel van wettelijke privacyrechten vastgesteld, waarin de toegang van rechtshandhavingsautoriteiten tot de inhoud van kabel-, mondeling of elektronisch communicatieverkeer dat door derden-providers wordt opgeslagen, is geregeld ([213]). Deze titel stelt de onrechtmatige toegang (d. w.z. niet toegestaan door een rechterlijke instantie of op andere wijze toelaatbaar) tot dergelijk communicatieverkeer strafbaar en biedt de getroffen natuurlijke persoon de mogelijkheid bij een Amerikaanse federale rechterlijke instantie een civielrechtelijke schadevordering alsook een vordering tot billijk of declaratoir herstel in te stellen tegen een overheidsfunctionaris die opzettelijk dergelijke onrechtmatige handelingen heeft verricht, of tegen de Verenigde Staten.

(117) Daarnaast bieden verschillende andere wetten natuurlijke personen het recht om tegen een Amerikaanse overheidsinstantie of functionaris een vordering in te stellen met betrekking tot de verwerking van hun persoonsgegevens, zoals de Wiretap Act ([214]), de Computer Fraud and Abuse Act ([215]), de Federal Torts Claim Act ([216]), de Right to Financial Privacy Act ([217]) en de Fair Credit Reporting Act ([218]).

([209]) 5 U.S.C. § 702.

([210]) Algemeen staat alleen tegen "definitieve" handelingen van de overheid — en niet tegen "voorlopige, procedurele of tussentijdse" handelingen van de overheid — gerechtelijk verhaal open. Zie 5 U.S.C. § 704.

([211]) 5 U.S.C. § 706, (2), (A).

([212]) 18 U.S.C. §§ 2701-2712.

([213]) De Electronic Communications Privacy Act beschermt communicatieverkeer bij twee welbepaalde klassen netwerkproviders, namelijk providers van: i) elektronische communicatiediensten, bijvoorbeeld telefonie of e-mail; ii) computerdiensten op afstand zoals opslag- of verwerkingsdiensten.

([214]) 18 U.S.C. §§ 2510 e.v. Op grond van de Wiretap Act (18 U.S.C. § 2520) kan een persoon van wie kabel-, mondeling of elektronisch communicatieverkeer is onderschept, openbaar is gemaakt of opzettelijk is gebruikt, een civielrechtelijke vordering wegens schending van de Wiretap Act instellen, onder meer — onder bepaalde omstandigheden — tegen een individuele overheidsfunctionaris of de Verenigde Staten. Zie voor het verzamelen van andere niet-inhoudelijke informatie (bv. IP-adres, in- en uitgaande e-mailadressen) ook het hoofdstuk "Pen Registers and Trap and Trace Devices" van titel 18 (18 U.S.C. §§ 3121-3127 en, voor civielrechtelijke vordering, § 2707).

([215]) 18 U.S.C. § 1030. Op grond van de Computer Fraud and Abuse Act kan een persoon een vordering instellen tegen eenieder met betrekking tot opzettelijke niet-toegestane toegang (of buiten de grenzen van de toegestane toegang) om informatie te verkrijgen van een financiële instelling, een computersysteem van de Amerikaanse overheid of een andere gespecificeerde computer, onder meer — onder bepaalde omstandigheden — tegen een individuele overheidsfunctionaris.

([216]) 28 U.S.C. §§ 2671 e.v. Op grond van de Federal Tort Claims Act kan een persoon — onder bepaalde omstandigheden — een vordering instellen tegen de Verenigde Staten met betrekking tot nalatig of onrechtmatig handelen of verzuim van alle personeelsleden van de overheid terwijl die binnen hun ambt of arbeidsovereenkomst optreden.

([217]) 12 U.S.C. §§ 3401 e.v. Op grond van de Right to Financial Privacy Act kan een persoon — onder bepaalde omstandigheden — een vordering instellen tegen de Verenigde Staten met betrekking tot het verkrijgen of het openbaar maken van beschermde financiële gegevens in strijd met de wet. Toegang van de overheid tot beschermde financiële gegevens is doorgaans verboden, tenzij de overheid een verzoek om een rechtmatig dwangbevel of huiszoekingsbevel indient of — onder bepaalde beperkingen — een formeel schriftelijk verzoek en de natuurlijke persoon van wie informatie wordt gevraagd, over dat verzoek wordt ingelicht.

([218]) 15 U.S.C. §§ 1681-1681x. Op grond van de Fair Credit Reporting Act kan een persoon een vordering instellen tegen eenieder die de vereisten (met name dat er een rechtmatige toestemming moet zijn) met betrekking tot het verzamelen, de verspreiding en het gebruik van consumentenkredietverslagen niet naleeft of — onder bepaalde omstandigheden — tegen een overheidsdienst.

(118) Op grond van de FOIA ([219]), 5 U.S.C. § 552, heeft eenieder tevens het recht op inzage van gegevens van federale instanties, ook wanneer die de persoonsgegevens van de natuurlijke persoon bevatten. Na uitputting van de administratieve procedures kan een natuurlijke persoon dat recht inroepen voor de rechter, tenzij die gegevens tegen openbaarmaking zijn beschermd op grond van een vrijstelling of een bijzondere uitzondering ten behoeve van de rechtshandhaving ([220]). In dat geval zal de rechter beoordelen of een vrijstelling van toepassing is of rechtmatig door de betrokken overheidsinstantie is ingeroepen.

3.2 **Toegang van en gebruik door de Amerikaanse overheidsdiensten ten behoeve van de nationale veiligheid**

(119) De Amerikaanse wetgeving omvat verschillende beperkingen en waarborgen met betrekking tot de toegang tot en het gebruik van persoonsgegevens met het oog op de nationale veiligheid, en voorziet in toezichts- en verhaalmechanismen op dit gebied die in overeenstemming zijn met de in overweging 89 van dit besluit bedoelde vereisten. De voorwaarden waaronder deze toegang kan plaatsvinden en de waarborgen die van toepassing zijn op het gebruik van deze bevoegdheden worden in de volgende punten in detail beoordeeld.

3.2.1 ***Rechtsgrondslagen, beperkingen en waarborgen***

3.2.1.1 *Toepasselijk rechtskader*

(120) Persoonsgegevens die vanuit de Unie worden doorgegeven aan EU-VS-DPF-organisaties kunnen door de Amerikaanse autoriteiten ten behoeve van de nationale veiligheid worden verzameld op basis van verschillende rechtsinstrumenten, met inachtneming van specifieke voorwaarden en waarborgen.

(121) Zodra persoonsgegevens zijn ontvangen door in de Verenigde Staten gevestigde organisaties, kunnen de inlichtingendiensten van de VS alleen toegang vragen tot die persoonsgegevens ten behoeve van de nationale veiligheid als dit bij wet is toegestaan, met name op grond van de Foreign Intelligence Surveillance Act (FISA) of wettelijke bepalingen die toegang toestaan door middel van *national security letters* (NSL) ([221]). De FISA bevat verscheidene rechtsgrondslagen die kunnen worden gebruikt om de persoonsgegevens te verzamelen (en vervolgens te verwerken) van betrokkenen uit de Unie die in het kader van het EU-VS-DPF worden doorgegeven (sectie 105 FISA ([222]), sectie 302 FISA ([223]), sectie 402 FISA ([224]), sectie 501 FISA ([225]) en sectie 702 FISA ([226])), zoals nader beschreven in de overwegingen 142 tot en met 152.

([219]) 5 U.S.C. § 552.

([220]) Die uitzonderingen zijn echter afgebakend. Overeenkomstig 5 U.S.C. § 552 (b), (7), bijvoorbeeld niet voor gegevens of informatie die ten behoeve van de rechtshandhaving worden verzameld, doch alleen in de mate waarin de mededeling van die gegevens of informatie a) naar verwachting redelijkerwijs handhavingsprocedures zou kunnen belemmeren, b) een persoon het recht op een eerlijk proces of een onpartijdige uitspraak zou kunnen ontnemen, c) naar verwachting redelijkerwijs een ongerechtvaardigde inbreuk op de persoonlijke privacy zou kunnen vormen, d) naar verwachting redelijkerwijs de identiteit van een vertrouwelijke bron openbaar zou kunnen maken, waaronder staats-, lokale of buitenlandse diensten of autoriteiten of particuliere instellingen die informatie op vertrouwelijke basis hebben verstrekt, en, in het geval van gegevens of informatie die in de loop van een strafonderzoek door een rechtshandhavingsautoriteit of door een dienst die rechtmatig inlichtingenwerk ten behoeve van de nationale veiligheid verricht, zijn verzameld, de identiteit van een vertrouwelijke bron die informatie heeft verstrekt, e) de technieken en procedures voor rechtshandhavingsonderzoeken openbaar zou maken, of de richtsnoeren voor rechtshandhavingsonderzoeken of -vervolgingen, als die openbaarmaking naar verwachting redelijkerwijs tot omzeiling van de wet zou kunnen leiden, of f) naar verwachting redelijkerwijs het leven of de fysieke veiligheid van een persoon in gevaar zou kunnen brengen. Daarnaast is het zo dat telkens wanneer een verzoek wordt gedaan met betrekking tot toegang tot gegevens [waarvan de mededeling naar verwachting redelijkerwijs handhavingsprocedures zou kunnen belemmeren] en a) het onderzoek of de procedure een mogelijke schending van de strafwet betreft, en b) er reden is om aan te nemen dat i) het onderwerp van het onderzoek of de procedure zich niet van het bestaan daarvan bewust is, en ii) openbaarmaking van het bestaan van de gegevens naar verwachting redelijkerwijs de handhavingsprocedures zou kunnen belemmeren, de dienst de gegevens mag behandelen als niet onderworpen aan de vereisten van deze sectie, doch alleen zolang die omstandigheid blijft duren. (5 U.S.C. § 552 , (c), (1)).

([221]) 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; alsmede 18 U.S.C. § 2709. Zie overweging 153.

([222]) 50 U.S.C. § 1804, dat betrekking heeft op traditioneel geïndividualiseerd elektronisch toezicht.

([223]) 50 U.S.C. § 1822, dat betrekking heeft op fysieke huiszoekingen ten behoeve van buitenlandse inlichtingen.

([224]) 50 U.S.C. § 1842 met § 1841(2) en sectie 3127 van titel 18, in verband met de installatie van een *pen register* of een *trap and trace device* (trackers van berichtenverkeer).

([225]) 50 U.S.C. § 1861, op grond waarvan de FBI een aanvraag kan indienen voor een bevel waarbij een gewone vervoerder, een openbare accommodatie, een faciliteit voor fysieke opslag of een faciliteit voor de verhuur van voertuigen wordt gemachtigd om gegevens in zijn of haar bezit vrij te geven voor een onderzoek om informatie over buitenlandse inlichtingen te verzamelen of voor een onderzoek naar internationaal terrorisme.

([226]) 50 U.S. Code § 1881a, op grond waarvan onderdelen van de Amerikaanse inlichtingendiensten toegang kunnen krijgen tot informatie, met inbegrip van de inhoud van internetcommunicatie, van Amerikaanse bedrijven, gericht op bepaalde niet-Amerikanen buiten de Verenigde Staten met de wettelijk verplichte hulp van aanbieders van elektronische communicatie.

(122) Inlichtingendiensten van de VS beschikken ook over mogelijkheden om persoonsgegevens buiten de Verenigde Staten te verzamelen, waaronder mogelijk persoonsgegevens in doorvoer tussen de Unie en de Verenigde Staten. De inzameling buiten de Verenigde Staten is gebaseerd op Executive Order 12333 (EO 12333) ([227]), uitgevaardigd door de president ([228]).

(123) Het verzamelen van SIGINT is de vorm van inlichtingenverzameling die het meest relevant is voor deze vaststelling van adequaatheid, aangezien het gaat om het verzamelen van elektronische communicatie en gegevens uit informatiesystemen. Deze verzameling kan worden uitgevoerd door de Amerikaanse inlichtingendiensten, zowel binnen de Verenigde Staten (op basis van de FISA) als tijdens de doorvoer van gegevens naar de Verenigde Staten (op basis van EO 12333).

(124) Op 7 oktober 2022 heeft de Amerikaanse president EO 14086 over de versterking van de waarborgen voor de Amerikaanse SIGINT uitgevaardigd, waarin beperkingen en waarborgen voor alle Amerikaanse SIGINT-activiteiten zijn vastgelegd. Dit EO vervangt grotendeels *Presidential Policy Directive 28*(presidentiële beleidsrichtlijn 28, hierna "PPD-28") ([229]) en versterkt de voorwaarden, beperkingen en waarborgen die gelden voor alle SIGINT-activiteiten (namelijk op grond van FISA en EO 12333), ongeacht waar deze plaatsvinden ([230]), en stelt een nieuw verhaalmechanisme in waarmee deze waarborgen kunnen worden ingeroepen en afgedwongen door natuurlijke personen ([231]) (zie meer in detail de overwegingen 176 tot en met 194). Aldus wordt het resultaat van de besprekingen tussen de EU en de VS na de nietigverklaring door het Hof van het besluit van de Commissie over de adequaatheid van het privacyschild (zie overweging 6) omgezet in Amerikaans recht. Het is derhalve een bijzonder belangrijk element van het in dit besluit beoordeelde rechtskader.

(125) De bij EO 14086 ingevoerde beperkingen en waarborgen vormen een aanvulling op de beperkingen en waarborgen die zijn bepaald in sectie 702 FISA en EO 12333. De hieronder (in de punten 3.2.1.2 en 3.2.1.3) beschreven voorschriften moeten door de inlichtingendiensten worden nageleefd wanneer zij SIGINT-activiteiten verrichten uit hoofde van sectie 702 FISA en EO 12333, bv. wanneer zij categorieën buitenlandse inlichtingen selecteren/aanwijzen die uit hoofde van sectie 702 FISA moeten worden verkregen; wanneer zij buitenlandse inlichtingen of contra-inlichtingen verzamelen uit hoofde van EO 12333; en wanneer zij besluiten nemen met betrekking tot het specificeren van een individueel doelwit uit hoofde van sectie 702 FISA en EO 12333.

(126) De in dit Executive Order van de president neergelegde vereisten zijn bindend voor alle inlichtingendiensten. Ze moeten verder worden uitgevoerd via beleidsmaatregelen en procedures van de instanties die ze omzetten in concrete aanwijzingen voor dagelijkse operaties. In dit verband geeft EO 14086 de Amerikaanse inlichtingendiensten maximaal een jaar de tijd om hun bestaande beleidsmaatregelen en procedures bij te werken (d.w.z. uiterlijk 7 oktober 2023) en in overeenstemming te brengen met de eisen van het EO. Dergelijke bijgewerkte beleidsmaatregelen en procedures moeten worden ontwikkeld in overleg met de minister van Justitie, de *Civil Liberties Protection Officer* (functionaris voor de bescherming van de burgerlijke vrijheden, hierna "CLPO") van het *Office of the Director of National Intelligence* (bureau van de directeur van de nationale inlichtingendienst, hierna "ODNI") en de PCLOB — een onafhankelijk toezichtsorgaan dat bevoegd is om het beleid van de uitvoerende macht en de uitvoering ervan te toetsen met het oog op de bescherming van de privacy en de burgerlijke vrijheden (zie overweging 110 voor de rol en het statuut van de PCLOB) — en openbaar worden gemaakt ([232]). Bovendien zal de PCLOB, zodra de bijgewerkte beleidslijnen en procedures zijn ingevoerd, een evaluatie uitvoeren om ervoor te

([227]) EO 12333: United States Intelligence Activities (inlichtingenactiviteiten van de Verenigde Staten), Federal Register vol. 40, nr. 235 (8 december 1981, zoals gewijzigd op 30 juli 2008). EO 12333 bevat een omschrijving van de doelstellingen, aanwijzingen, taken en verantwoordelijkheden van het Amerikaanse inlichtingenwerk (met inbegrip van de rol van de verschillende onderdelen van de inlichtingendiensten) en legt de algemene parameters voor de uitvoering van inlichtingenactiviteiten vast.

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

([229]) EO 14086 vervangt een eerdere presidentiële richtlijn, PPD-28, met uitzondering van sectie 3 en een aanvullende bijlage (die inlichtingendiensten verplicht jaarlijks hun prioriteiten en behoeften op het gebied van SIGINT te evalueren, rekening houdend met de voordelen van SIGINT-activiteiten voor de nationale belangen van de VS en met het aan die activiteiten verbonden risico) en sectie 6 (die algemene bepalingen bevat), zie het memorandum over de nationale veiligheid betreffende de gedeeltelijke intrekking van presidentiële beleidsrichtlijn 28 beschikbaar op https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/

([230]) Zie sectie 5(f) EO 14086, waarin wordt uitgelegd dat het EO hetzelfde toepassingsgebied heeft als PPD-28, dat, volgens voetnoot 3, van toepassing was op SIGINT-activiteiten die worden verricht om communicatie of informatie over communicatie te verzamelen, met uitzondering van SIGINT-activiteiten die worden verricht om SIGINT-capaciteiten te testen of te ontwikkelen.

([231]) Zie in dit verband bijvoorbeeld sectie 5(h) EO 14086, waarin wordt verduidelijkt dat de waarborgen in het EO een wettelijk recht creëren en door natuurlijke personen kunnen worden afgedwongen via het verhaalmechanisme.

([232]) Zie sectie 2, (c), (iv), (C), EO 14086.

zorgen dat zij in overeenstemming zijn met het EO. Binnen 180 dagen na afronding van een dergelijke evaluatie door de PCLOB moet elke inlichtingendienst alle aanbevelingen van de PCLOB zorgvuldig overwegen en uitvoeren of anderszins aanpakken. Op 3 juli 2023 heeft de Amerikaanse overheid dergelijke bijgewerkte beleidsmaatregelen en procedures bekendgemaakt ([233]).

3.2.1.2 *Beperkingen en waarborgen met betrekking tot het verzamelen van persoonsgegevens ten behoeve van de nationale veiligheid*

(127) EO 14086 stelt een aantal verregaande eisen die gelden voor alle SIGINT-activiteiten (verzamelen, gebruiken, verspreiden enz. van persoonsgegevens).

(128) Ten eerste moeten deze activiteiten gebaseerd zijn op een wet of een presidentiële machtiging en plaatsvinden in overeenstemming met het Amerikaanse recht, met inbegrip van de grondwet ([234]).

(129) Ten tweede moeten er passende waarborgen zijn om ervoor te zorgen dat de privacy en burgerlijke vrijheden integraal deel uitmaken van de planning van dergelijke activiteiten ([235]).

(130) Met name mogen SIGINT-activiteiten alleen worden uitgevoerd nadat op basis van een redelijke beoordeling van alle relevante factoren is vastgesteld dat de activiteiten noodzakelijk zijn om een gevalideerde inlichtingenprioriteit te bevorderen (zie overweging 135 voor het begrip "gevalideerde inlichtingenprioriteit") ([236]).

(131) Bovendien mogen dergelijke activiteiten alleen worden uitgevoerd in de mate en op een wijze die evenredig is aan de gevalideerde prioriteit van de inlichtingen waarvoor zij zijn toegestaan ([237]). Met andere woorden, er moet een juist evenwicht worden gevonden tussen het belang van de nagestreefde inlichtingenprioriteit en de gevolgen voor de privacy en de burgerlijke vrijheden van de betrokken personen, ongeacht hun nationaliteit of de plaats waar zij verblijven ([238]).

(132) Om te waarborgen dat deze algemene eisen — die de beginselen van wettigheid, noodzakelijkheid en evenredigheid weerspiegelen — worden nageleefd, zijn de SIGINT-activiteiten onderworpen aan toezicht (zie meer in detail sectie 3.2.2) ([239]).

(133) Deze overkoepelende vereisten worden met betrekking tot het verzamelen van SIGINT verder onderbouwd met een aantal voorwaarden en beperkingen die ervoor zorgen dat de inmenging in de rechten van natuurlijke personen beperkt blijft tot hetgeen noodzakelijk en evenredig is om een legitiem doel te bereiken.

(134) Ten eerste beperkt het EO op twee manieren de gronden waarop gegevens kunnen worden verzameld in het kader van SIGINT-activiteiten. Enerzijds legt het EO de legitieme doelstellingen vast die kunnen worden nagestreefd met het verzamelen van SIGINT, bijvoorbeeld om de vermogens, bedoelingen of activiteiten te begrijpen of te beoordelen van buitenlandse organisaties, met inbegrip van internationale terroristische organisaties, die een actuele of potentiële bedreiging vormen voor de nationale veiligheid van de Verenigde Staten; om te beschermen tegen buitenlandse militaire vermogens en activiteiten; om transnationale bedreigingen te begrijpen of te beoordelen die van invloed zijn op de mondiale veiligheid, zoals klimaatverandering en andere ecologische veranderingen, risico's voor de volksgezondheid en humanitaire bedreigingen ([240]). Anderzijds somt het EO bepaalde doelstellingen op die

([233]) https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086.

([234]) Sectie 2, (a), (i), EO 14086.

([235]) Sectie 2, (a), (ii), EO 14086.

([236]) Sectie 2, (a), (ii), (A), EO 14086. Dit vereist niet altijd dat SIGINT het enige middel zijn om aspecten van een gevalideerde inlichtingenprioriteit te bevorderen. Het verzamelen van SIGINT kan bijvoorbeeld worden gebruikt om alternatieve routes voor validering te garanderen (bijvoorbeeld om informatie uit andere inlichtingenbronnen te bevestigen) of om betrouwbare toegang tot dezelfde informatie te behouden (sectie 2, (c), (i), (A), EO 14086).

([237]) Sectie 2, (a), (ii), (B), EO 14086.

([238]) Sectie 2, (a), (ii), (B), EO 14086.

([239]) Sectie 2, (a), (iii), in samenhang met sectie 2, (d), EO 14086.

([240]) Sectie 2, (b), (i), EO 14086. Omdat de lijst van legitieme doelstellingen in de EO is afgebakend en mogelijke toekomstige dreigingen daarin niet zijn opgenomen, voorziet de EO in de mogelijkheid dat de president deze lijst bijwerkt als zich nieuwe vereisten in verband met de nationale veiligheid, zoals nieuwe bedreigingen voor de nationale veiligheid, voordoen. Deze bijwerkingen moeten in beginsel openbaar worden gemaakt, tenzij de president bepaalt dat dit zelf een risico voor de nationale veiligheid van de Verenigde Staten zou vormen (sectie 2, (b), (i), (B), EO 14086).

nooit mogen worden nagestreefd met SIGINT-activiteiten, bijvoorbeeld om kritiek, afwijkende meningen of de vrije uiting van ideeën of politieke meningen door personen of de pers te belemmeren; om personen te benadelen op grond van hun etniciteit, ras, geslacht, genderidentiteit, seksuele geaardheid of godsdienst; of om Amerikaanse bedrijven een concurrentievoordeel te geven ([241]).

(135) Bovendien kunnen de in EO 14086 vastgelegde legitieme doelstellingen op zichzelf door de inlichtingendiensten niet worden ingeroepen om het verzamelen van SIGINT te rechtvaardigen, maar moeten deze voor operationele doeleinden verder worden uitgewerkt tot concretere prioriteiten waarvoor SIGINT kunnen worden verzameld. Met andere woorden, de feitelijke verzameling kan alleen plaatsvinden om een specifiekere prioriteit te bevorderen. Die prioriteiten worden vastgesteld via een specifiek proces dat gericht is op de naleving van de toepasselijke wettelijke voorschriften, waaronder die betreffende privacy en burgerlijke vrijheden. Meer bepaald worden inlichtingenprioriteiten eerst uitgewerkt door de *Director of National Intelligence* (via het zogenaamde *National Intelligence Priorities Framework* — "kader voor de nationale inlichtingenprioriteiten") en ter goedkeuring voorgelegd aan de president ([242]). Alvorens inlichtingenprioriteiten aan de president voor te stellen, moet de directeur, overeenkomstig EO 14086, voor elke prioriteit een beoordeling krijgen van de CLPO van het ODNI over de vraag of deze 1) een of meer in het EO genoemde legitieme doelstellingen bevordert; 2) niet is bedoeld voor of naar verwachting zal resulteren in het verzamelen van SIGINT voor een in het EO genoemd verboden doel; en 3) is vastgesteld met inachtneming van de privacy en de burgerlijke vrijheden van alle personen, ongeacht hun nationaliteit of verblijfplaats ([243]). Indien de directeur het niet eens is met de beoordeling van de CLPO, moeten beide standpunten worden voorgelegd aan de president ([244]).

(136) Daarom zorgt dit proces er met name voor dat met privacyoverwegingen rekening wordt gehouden vanaf het eerste stadium waarin de inlichtingenprioriteiten worden uitgewerkt.

(137) Ten tweede, wanneer eenmaal een inlichtingenprioriteit is vastgesteld, wordt aan de hand van een aantal vereisten beslist of en in hoeverre ter bevordering van die prioriteit SIGINT mag worden verzameld. Deze vereisten operationaliseren de overkoepelende noodzakelijkheids- en evenredigheidsnormen van sectie 2, (a) van het EO.

(138) Met name mogen SIGINT alleen worden verzameld nadat op basis van een redelijke beoordeling van alle relevante factoren is vastgesteld dat de verzameling noodzakelijk is om een specifieke inlichtingenprioriteit te bevorderen ([245]). Bij het bepalen of een specifieke activiteit voor het verzamelen van SIGINT nodig is om een gevalideerde inlichtingenprioriteit te bevorderen, moeten de Amerikaanse inlichtingendiensten de beschikbaarheid, haalbaarheid en geschiktheid van andere, minder ingrijpende bronnen en methoden, waaronder diplomatieke en openbare bronnen, in overweging nemen ([246]). Indien beschikbaar moeten dergelijke alternatieve, minder ingrijpende bronnen en methoden voorrang krijgen ([247]).

(139) Wanneer bij de toepassing van dergelijke criteria het verzamelen van SIGINT noodzakelijk wordt geacht, moet dit zo gericht mogelijk plaatsvinden en mag het geen onevenredige gevolgen hebben voor de privacy en de burgerlijke vrijheden ([248]). Om ervoor te zorgen dat de privacy en de burgerlijke vrijheden niet onevenredig worden aangetast — d.w.z. om een juist evenwicht te vinden tussen de behoeften inzake de nationale veiligheid en de bescherming van de privacy en de burgerlijke vrijheden — moet naar behoren rekening worden gehouden met alle relevante factoren, zoals de aard van het nagestreefde doel; de indringendheid van de verzamelactiviteit, met inbegrip van de duur ervan; de waarschijnlijke bijdrage van de verzameling aan het nagestreefde doel; de redelijkerwijs voorzienbare gevolgen voor natuurlijke personen; en de aard en gevoeligheid van de te verzamelen gegevens ([249]).

([241]) Sectie 2, (b), (ii), EO 14086.
([242]) Sectie 102A van de National Security Act en sectie 2, (b), (iii), EO 14086.
([243]) In uitzonderlijke gevallen (met name wanneer een dergelijk proces niet kan worden uitgevoerd omdat moet worden voorzien in een nieuwe of zich ontwikkelende behoefte aan inlichtingen) kunnen deze prioriteiten rechtstreeks worden vastgesteld door de president of het hoofd van een onderdeel van de inlichtingendiensten, die in beginsel dezelfde criteria moeten toepassen als die welke zijn beschreven in sectie 2, (b), (iii), (A), (1)-(3), zie sectie 4, (n), EO 14086.
([244]) Sectie 2, (b), (iii), (C), EO 14086.
([245]) Sectie 2, (b) en (c), (i), (A), EO 14086.
([246]) Sectie 2, (c), (i), (A), EO 14086.
([247]) Sectie 2, (c), (i), (A), EO 14086.
([248]) Sectie 2, (c), (i), (B), EO 14086.
([249]) Sectie 2, (c), (i), (B), EO 14086.

(140) Wat de aard van de verzameling van SIGINT betreft, moet de verzameling van gegevens binnen de Verenigde Staten, die voor deze vaststelling van adequaatheid het meest relevant is omdat het gaat om gegevens die zijn doorgegeven aan organisaties in de VS, altijd gericht zijn, zoals in de overwegingen 142 tot en met 153 nader wordt toegelicht.

(141) "Bulksgewijze verzameling" ([250]) kan alleen worden verricht buiten de Verenigde Staten, op grond van EO 12333. Ook in dit geval moet overeenkomstig EO 14086 prioriteit worden gegeven aan gerichte verzameling ([251]). Omgekeerd is bulksgewijze verzameling alleen toegestaan wanneer de informatie die nodig is om een gevalideerde inlichtingenprioriteit te bevorderen, redelijkerwijs niet kan worden verkregen door gerichte verzameling ([252]). Wanneer gegevens bulksgewijs buiten de Verenigde Staten moeten worden verzameld, zijn de specifieke waarborgen van EO 14086 van toepassing ([253]). Ten eerste moeten methoden en technische maatregelen worden toegepast om de verzamelde gegevens te beperken tot wat nodig is om een gevalideerde inlichtingenprioriteit te bevorderen, terwijl het verzamelen van niet-relevante informatie tot een minimum wordt beperkt ([254]). Ten tweede beperkt het EO het gebruik van bulksgewijs verzamelde informatie (inclusief bevraging) tot zes specifieke doelstellingen, waaronder bescherming tegen terrorisme, gijzeling en het gevangen houden van personen door of namens een buitenlandse regering, organisatie of persoon; bescherming tegen buitenlandse spionage, sabotage of moord; bescherming tegen bedreigingen in verband met de ontwikkeling, het bezit of de verspreiding van massavernietigingswapens of daarmee verband houdende technologieën en bedreigingen enz. ([255]). Ten slotte mogen bulksgewijs verzamelde SIGINT alleen worden doorzocht wanneer dat nodig is om een gevalideerde inlichtingenprioriteit te bevorderen, ter verwezenlijking van deze zes doelstellingen en in overeenstemming met beleid en procedures die op passende wijze rekening houden met het effect van de doorzoekingen op de privacy en de burgerlijke vrijheden van alle personen, ongeacht hun nationaliteit of verblijfplaats ([256]).

(142) Naast de vereisten van EO 14086 is het verzamelen via SIGINT van gegevens die zijn doorgegeven aan een organisatie in de Verenigde Staten onderworpen aan specifieke beperkingen en waarborgen die worden geregeld in sectie 702 FISA ([257]). Sectie 702 FISA maakt het mogelijk buitenlandse inlichtingen te verzamelen door niet-Amerikanen van wie redelijkerwijs mag worden aangenomen dat zij zich buiten de Verenigde Staten bevinden, te specificeren als doelwit, met de gedwongen ondersteuning van Amerikaanse aanbieders van elektronische-communicatiediensten ([258]). Om overeenkomstig sectie 702 FISA buitenlandse inlichtingen te kunnen verzamelen,

([250]) M.a.w. de verzameling van grote hoeveelheden SIGINT die om technische of operationele redenen worden verkregen zonder gebruik van discriminanten (bijvoorbeeld zonder gebruik van specifieke identificatoren of selectietermen), zie sectie 4, (b), EO 14086. Overeenkomstig EO 14086 en zoals nader toegelicht in overweging 141, vindt bulksgewijze verzameling uit hoofde van EO 12333 alleen plaats wanneer dat nodig is om specifieke gevalideerde inlichtingenprioriteiten te bevorderen, en is zij onderworpen aan een aantal beperkingen en waarborgen die ervoor moeten zorgen dat gegevens niet ongedifferentieerd worden opgevraagd. Bulksgewijze verzameling moet derhalve worden onderscheiden van verzameling op algemene en ongedifferentieerde basis ("massasurveillance") zonder beperkingen en waarborgen.

([251]) Sectie 2, (c), (ii), (A), EO 14086.

([252]) Sectie 2, (c), (ii), (A), EO 14086.

([253]) De specifieke regels van EO 14086 inzake de bulksgewijze verzameling van gegevens zijn ook van toepassing op gerichte activiteiten in het kader van de verzameling van SIGINT waarbij tijdelijk gebruik wordt gemaakt van gegevens zonder discriminanten (bv. specifieke selectietermen of identificatoren), d.w.z. in bulk (hetgeen uitsluitend mogelijk is buiten het grondgebied van de Verenigde Staten). Dit is niet het geval wanneer die gegevens uitsluitend worden gebruikt ter ondersteuning van de eerste technische fase van de gerichte verzameling van SIGINT, slechts worden bijgehouden gedurende de korte periode die nodig is om deze fase te voltooien en onmiddellijk daarna worden gewist (sectie 2, (c), (ii), (D), EO 14086). In dit geval heeft de eerste verzameling zonder discriminanten uitsluitend tot doel een gerichte verzameling van informatie mogelijk te maken door een specifieke idenitificator of selectieterm toe te passen. In een dergelijk scenario worden alleen gegevens die reageren op de toepassing van een bepaalde discriminant in overheids-databanken opgenomen, terwijl de overige gegevens worden vernietigd. Voor deze gerichte verzameling blijven derhalve de algemene regels van toepassing die gelden voor de verzameling van SIGINT, waaronder sectie 2, (a)-(b) en 2, (c), (i), EO 14086.

([254]) Sectie 2, (c), (ii), (A), EO 14086.

([255]) Sectie 2, (c), (ii), (B), EO 14086. Indien zich nieuwe vereisten n verband met de nationale veiligheid voordoen, zoals nieuwe bedreigingen voor de nationale veiligheid, kan de president deze lijst bijwerken. Deze bijwerkingen moeten in beginsel openbaar worden gemaakt, tenzij de president bepaalt dat dit zelf een risico voor de nationale veiligheid van de Verenigde Staten zou vormen (sectie 2, (c), (ii), (C), EO 14086). Wat betreft het doorzoeken van bulksgewijs verzamelde gegevens, zie sectie 2, (c), (iii), (D), EO 14086.

([256]) Sectie 2, (a), (ii), (A), in samenhang met sectie 2, (c), (iii), (D), EO 14086. Zie ook bijlage VII.

([257]) 50 U.S.C. § 1881.

([258]) 50 U.S.C. § 1881a (a). Zoals de PCLOB opmerkt, bestaat surveillance op grond van sectie 702 volledig uit het specificeren als doelwit van specifieke [niet-Amerikaanse] personen over wie een geïndividualiseerd besluit is genomen (Privacy and Civil Liberties Oversight Board,"Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" [Verslag over het surveillanceprogramma uit hoofde van sectie 702 van de Foreign Intelligence Surveillance Act], 2 juli 2014, verslag uit hoofde van sectie 702, blz. 111). Zie Civil Liberties and Privacy Office van de NSA, "NSA's Implementation of Foreign Intelligence Surveillance Act Section 702" [De tenuitvoerlegging van sectie 702 van de Foreign Intelligence Surveillance Act door de NSA], 16 april 2014. De term "aanbieder van elektronische-communicatiediensten" is gedefinieerd in 50 U.S.C. § 1881 (a)(4).

dienen de minister van Justitie en de Director of National Intelligence jaarlijks verklaringen in bij de *Foreign Intelligence Surveillance Court* (FISC) waarin categorieën van te verwerven buitenlandse inlichtingen worden vastgesteld ([259]). De certificeringen moeten vergezeld gaan van procedures om het doelwit te specificeren, minimaliseringsprocedures en procedures voor het doorzoeken, die ook door de FISC worden goedgekeurd en juridisch bindend zijn voor de Amerikaanse inlichtingendiensten.

(143) De FISC is een onafhankelijke rechterlijke instantie ([260]) die bij federale wet is ingesteld. Tegen de beslissingen ervan kan beroep worden ingesteld bij de *Foreign Intelligence Surveillance Court of Review* (FISCR) ([261]) en in laatste instantie bij het Hooggerechtshof van de Verenigde Staten ([262]). De FISC (en de FISCR) worden ondersteund door een permanent panel van vijf juristen en vijf technische deskundigen die beschikken over deskundigheid op het gebied van nationale veiligheid en de burgerlijke vrijheden ([263]). De FISC benoemt uit deze groep een persoon als *amicus curiae* om te helpen bij de behandeling van verzoeken om een bevel of onderzoek die, volgens de FISC, een nieuwe of belangrijke uitlegging van het recht behelzen, tenzij de FISC oordeelt dat een dergelijke benoeming niet passend is ([264]). Hierdoor wordt met name gewaarborgd dat in de beoordeling van de FISC privacyoverwegingen naar behoren in aanmerking worden genomen. Ook kan de FISC als *amicus curiae* een persoon of organisatie aanwijzen die onder meer technische deskundigheid verschaft, wanneer dit wenselijk wordt geacht, of op verzoek een persoon of organisatie toestemming verlenen om als *amicus curiae* opmerkingen in te dienen ([265]).

(144) De FISC toetst de certificeringen en de bijbehorende procedures (met name de procedures om het doelwit te specificeren en de minimaliseringsprocedures) aan de vereisten van de FISA. Indien de FISC vaststelt dat niet aan de vereisten is voldaan, kan zij de certificering geheel of gedeeltelijk afwijzen en eisen dat de procedures worden gewijzigd ([266]). In dit verband heeft de FISC herhaaldelijk bevestigd dat haar toetsing van de procedures om het doelwit te specificeren en de minimaliseringsprocedures uit hoofde van sectie 702 niet beperkt blijft tot de procedures zoals deze zijn neergeschreven, maar ook betrekking heeft op de wijze waarop de procedures door de overheid worden uitgevoerd ([267]).

(145) De National Security Agency (NSA, de inlichtingendienst die krachtens sectie 702 FISA verantwoordelijk is voor targeting) stelt individuele doelwitten vast overeenkomstig door de FISC goedgekeurde procedures voor het specificeren van doelwitten, waarbij de NSA op basis van het geheel van de omstandigheden moet beoordelen of het specificeren van een specifieke persoon als doelwit waarschijnlijk leidt tot het verkrijgen van een categorie van buitenlandse inlichtingen die in een certificering zijn omschreven ([268]). Deze beoordeling moet specifiek en op feiten gebaseerd zijn, op grond van het analytisch oordeel, de gespecialiseerde opleiding en ervaring van de analist en de

([259]) 50 U.S.C. § 1881a (g).

([260]) De FISC bestaat uit rechters die door de *Chief Justice* van de Verenigde Staten zijn benoemd uit de zittende rechters van *district courts*, die eerder door de president zijn benoemd en door de Senaat zijn bevestigd. De rechters zijn voor het leven benoemd, kunnen alleen om gegronde redenen uit hun ambt worden gezet en werken voor de FISC voor een termijn van zeven jaar volgens een systeem van gespreide benoemingen. De FISA schrijft voor dat de rechters uit ten minste zeven verschillende *judicial circuits* van de Verenigde Staten moeten komen. Zie 50 U.S.C. § 1803 (a). De rechters worden ondersteund door ervaren justitiële medewerkers die het juridisch personeel van de rechtbank vormen en juridische analyses voorbereiden inzake verzoeken om verzameling. Zie de brief van de Honourable Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, aan de Honourable Patrick J. Leahy, voorzitter, Committee on the Judiciary, Amerikaanse Senaat (29 juli 2013) (hierna "de Walton-brief" genoemd), blz. 2, beschikbaar op https://fas.org/irp/news/2013/07/fisc-leahy.pdf

([261]) De FISCR bestaat uit rechters die door de *Chief Justice* van de Verenigde Staten zijn benoemd en uit *district courts* of *courts of appeal* van de Verenigde Staten komen, voor een termijn van zeven jaar volgens een systeem van gespreide benoemingen. Zie 50 U.S.C. § 1803 (b).

([262]) Zie 50 U.S.C. § 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i), (4).

([263]) 50 U.S.C. § 1803 (i), (1), (3), (A).

([264]) 50 U.S.C. § 1803 (i), (2), (A).

([265]) 50 U.S.C. § 1803 (i), (2), (B).

([266]) Zie bijvoorbeeld het advies van de FISC van 18 oktober 2018, beschikbaar op https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, zoals bevestigd door de Foreign Intelligence Court of Review in haar advies van 12 juli 2019, beschikbaar op https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12 Jul19.pdf

([267]) Zie bijvoorbeeld FISC, "Memorandum Opinion and Order", blz. 35 (18 november 2020) (goedgekeurd voor openbare bekendmaking op 26 april 2021), (bijlage D).

([268]) 50 U.S.C. § 1881a(a), "Procedures used by the National Security Agency for Targeting Non-United States Persons Reasonably Believe to be Located outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978" [Procedures van de National Security Agency voor het specificeren als doelwit van niet-Amerikanen van wie redelijkerwijs mag worden aangenomen dat zij zich buiten de Verenigde Staten bevinden, teneinde buitenlandse inlichtingen te verkrijgen overeenkomstig sectie 702 van de Foreign Intelligence Surveillance Act van 1978], zoals gewijzigd, van maart 2018 (procedures voor het specificeren van doelwitten van de NSA), beschikbaar op https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27 Mar18.pdf, blz. 1-4, verder toegelicht in het verslag van de PCLOB, blz. 41-42.

aard van de te verkrijgen buitenlandse inlichtingen ([269]). Het vaststellen van doelwitten wordt uitgevoerd door zogenaamde selectietermen die specifieke communicatievoorzieningen identificeren, zoals het e-mailadres of telefoonnummer van het doelwit, maar nooit sleutelwoorden of namen van personen ([270]).

(146) Om te beginnen bepalen de analisten van de NSA niet-Amerikanen in het buitenland waarvoor surveillance volgens hun beoordeling zal leiden tot de in de certificering gespecificeerde relevante buitenlandse inlichtingen ([271]). Zoals uiteengezet in de procedures voor het specificeren van doelwitten van de NSA kan de NSA alleen surveillance op een doelwit richten wanneer zij reeds iets over het doelwit te weten is gekomen ([272]). Dit kan volgen uit informatie uit verschillende bronnen, bijvoorbeeld menselijke inlichtingen. Via deze andere bronnen moet de analist ook kennis nemen van een specifieke selectieterm (d.w.z. communicatieaccount) die door het potentiële doelwit wordt gebruikt. Nadat die individuele personen zijn bepaald en na het doorlopen van een uitgebreid evaluatiemechanisme binnen de NSA als doelwit zijn goedgekeurd ([273]), worden vervolgens de selectietermen bepaald die voor de identificatie van de door de doelwitten gebruikte communicatievoorzieningen (zoals e-mailadressen) zullen worden ingezet (d.w.z. ontwikkeld en toegepast) ([274]).

(147) De NSA moet de feitelijke basis voor het specificeren van het doelwit documenteren ([275]) en na de eerste specificatie als doelwit regelmatig bevestigen dat nog steeds aan de norm voor het specificeren van doelwitten wordt voldaan ([276]). Zodra niet langer aan de norm voor het specificeren van doelwitten wordt voldaan, moet het verzamelen worden stopgezet ([277]). De selectie van elk doelwit door de NSA en de registratie van elke geregistreerde doelwitbeoordeling en -motivering worden om de twee maanden gecontroleerd op naleving van de procedures voor het specificeren van doelwitten door ambtenaren van de bureaus voor toezicht op de inlichtingendiensten van het ministerie van Justitie, die verplicht zijn elke schending te melden aan de FISC en aan het Congres ([278]). De schriftelijke documentatie van de NSA vergemakkelijkt het toezicht van de FISC op de vraag of specifieke personen naar behoren als doelwit worden gespecificeerd, op grond van sectie 702 FISA, overeenkomstig de in de overwegingen 173-174 beschreven toezichtsbevoegdheden van de FISC ([279]). Ten slotte moet de Director of National Intelligence (DNI) ook elk jaar het totale aantal doelwitten uit hoofde van sectie 702 FISA rapporteren in openbare jaarlijkse statistische transparantieverslagen. Bedrijven die richtlijnen uit hoofde van sectie 702 FISA ontvangen, mogen geaggregeerde gegevens publiceren (via transparantieverslagen) over de verzoeken die zij ontvangen ([280]).

([269]) Procedures voor het specificeren van doelwitten van de NSA, blz. 4.

([270]) Zie Privacy and Civil Liberties Oversight Board, "Section 702 Report" (Verslag over sectie 702), blz. 32-33 en 45, met verdere verwijzingen. Zie ook "Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017" [Halfjaarlijkse beoordeling van de naleving van de procedures en richtsnoeren uit hoofde van sectie 702 van de Foreign Intelligence Surveillance Act, ingediend door de minister van Justitie en de Director of National Intelligence, verslagperiode: 1 december 2016 – 31 mei 2017], blz. 41 (oktober 2018), beschikbaar op: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf

([271]) Zie Privacy and Civil Liberties Oversight Board, "Section 702 Report" (Verslag over sectie 702), blz. 42-43.

([272]) Procedures voor het specificeren van doelwitten van de NSA, blz. 2.

([273]) Zie Privacy and Civil Liberties Oversight Board, "Section 702 Report" (Verslag over sectie 702), blz. 46. De NSA moet bijvoorbeeld nagaan of er een verband bestaat tussen het doelwit en de selectieterm, en de naar verwachting te verkrijgen buitenlandse inlichtingen documenteren. Die informatie moet worden beoordeeld en goedgekeurd door twee hoofdanalisten van de NSA, en het algehele proces zal worden gevolgd voor latere nalevingscontroles door het ODNI en het ministerie van Justitie. Zie Civil Liberties and Privacy Office van de NSA, "NSA's Implementation of Foreign Intelligence Surveillance Act Section 702" [De uitvoering van sectie 702 van de Foreign Intelligence Surveillance Act door de NSA], 16 april 2014.

([274]) 50 U.S.C. § 1881a (h).

([275]) Procedures voor het specificeren van doelwitten van de NSA, blz. 8. Zie ook Privacy and Civil Liberties Oversight Board, "Section 702 Report" (Verslag over sectie 702), blz. 46. Het niet verstrekken van een schriftelijke motivering vormt een incident in verband met de naleving van de documentatie, dat moet worden gemeld aan de FISC en het Congres. Zie "Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017" [Halfjaarlijkse beoordeling van de naleving van de procedures en richtsnoeren uit hoofde van sectie 702 van de Foreign Intelligence Surveillance Act, ingediend door de minister van Justitie en de Director of National Intelligence, verslagperiode: 1 december 2016 – 31 mei 2017], blz. 41 (oktober 2018), "DOJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017" [Nalevingsverslag DOJ/ODNI aan de FISC voor december 2016 - mei 2017], blz. A-6, beschikbaar op: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf

([276]) Zie "U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements" [Opmerkingen van de Amerikaanse regering aan het Foreign Intelligence Surveillance Court, 2015 — Samenvatting van de belangrijkste vereisten van sectie 702], blz. 2-3 (15 juli 2015) en de informatie in bijlage VII.

([277]) Zie "U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements" [Opmerkingen van de Amerikaanse regering aan het Foreign Intelligence Surveillance Court, 2015 — Samenvatting van de belangrijkste vereisten van sectie 702], blz. 2-3 (15 juli 2015), waarin wordt bepaald dat indien de overheid later oordeelt dat de voortzetting van de activering van de selectieterm voor een doelwit naar verwachting niet zal leiden tot de verkrijging van buitenlandse inlichtingen, onmiddellijke deactivering vereist is, en uitstel kan leiden tot een te rapporteren nalevingsincident. Zie ook de informatie in bijlage VII.

([278]) Zie Privacy and Civil Liberties Oversight Board, "Section 702 Report" (Verslag over sectie 702), blz. 70-72; Regel 13(b) van het Reglement van het United States Intelligence Surveillance Court, beschikbaar op https://www.fisc.uscourts.gov/sites/default/files/FISC Rules of Procedure.pdf

([279]) Zie ook "DOJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017" [Nalevingsverslag DOJ/ODNI aan de FISC voor december 2016 - mei 2017], blz. A-6.

([280]) 50 U.S.C. § 1874.

(148) Voor de andere rechtsgronden voor het verzamelen van persoonsgegevens die aan organisaties in de VS worden doorgegeven, gelden andere beperkingen en waarborgen. In het algemeen is het bulksgewijs verzamelen van gegevens uitdrukkelijk verboden krachtens sectie 402 FISA (*pen registers* en *trap and trace devices* (trackers van berichtenverkeer)) en via het gebruik van *national security letters*, en is het gebruik van specifieke "selectietermen" vereist ([281]).

(149) Om traditionele geïndividualiseerde elektronische surveillance uit te voeren (uit hoofde van sectie 105 FISA), moeten de inlichtingendiensten een aanvraag indienen bij de FISC met een verklaring van de feiten en omstandigheden die de overtuiging rechtvaardigen dat er een redelijk vermoeden is dat de faciliteit wordt gebruikt of op het punt staat te worden gebruikt door een buitenlandse mogendheid of een vertegenwoordiger van een buitenlandse mogendheid ([282]). De FISC zal onder andere beoordelen of er op basis van de voorgelegde feiten sprake is van een redelijk vermoeden dat dit inderdaad het geval is ([283]).

(150) Voor een huiszoeking die moet leiden tot een inspectie, inbeslagneming enz. van informatie, materiaal of eigendom (bv. een computer) op basis van sectie 301 FISA, is een verzoek om een bevel van de FISC vereist ([284]). In een dergelijk verzoek moet onder meer worden aangetoond dat er een redelijk vermoeden bestaat dat het doelwit van de huiszoeking een buitenlandse mogendheid of een vertegenwoordiger van een buitenlandse mogendheid is; dat de te doorzoeken ruimte of eigendom buitenlandse inlichtingen bevat en dat de te doorzoeken ruimte eigendom is van, gebruikt wordt door, in bezit is van of onderweg is naar of van een (vertegenwoordiger van een) buitenlandse mogendheid ([285]).

(151) Evenzo vereist de installatie van *pen registers* en *trap and trace devices* (trackers van berichtenverkeer) (overeenkomstig afdeling 402 FISA) een verzoek om een bevel van de FISC (of een Amerikaanse *magistrate judge*) en het gebruik van een specifieke selectieterm, d.w.z. een term die specifiek een persoon, account enz. aanduidt en wordt gebruikt om, voor zover redelijkerwijs mogelijk, de reikwijdte van de gezochte informatie te beperken ([286]). Deze bevoegdheid heeft geen betrekking op de inhoud van de communicatie, maar slaat op informatie over de klant of abonnee die van een dienst gebruikmaakt (zoals naam, adres, abonneenummer, soort/duur van de ontvangen dienst, bron/mechanisme van betaling).

(152) Sectie 501 FISA ([287]), die het verzamelen van bedrijfsgegevens van een openbaarvervoerbedrijf (d.w.z. een persoon of entiteit die tegen vergoeding personen of goederen vervoert over land, per spoor, over het water of door de lucht), een openbare accommodatie (bv. een hotel, motel of herberg), een autoverhuurbedrijf of een fysieke opslagplaats (d. w.z. die ruimte biedt voor of diensten verleent in verband met de opslag van goederen en materialen) toestaat ([288]), vereist ook een aanvraag bij de FISC of een *magistrate judge*. In dit verzoek moeten de opgevraagde gegevens worden vermeld alsmede de specifieke en concrete feiten op grond waarvan kan worden aangenomen dat de persoon op wie de gegevens betrekking hebben een buitenlandse mogendheid of een vertegenwoordiger van een buitenlandse mogendheid is ([289]).

(153) *National security letters*, ten slotte, zijn volgens verschillende wetten toegestaan en stellen onderzoeksinstanties in staat van bepaalde entiteiten (bv. financiële instellingen, kredietinformatiebureaus, aanbieders van elektronische communicatie) bepaalde informatie (met uitzondering van de inhoud van de communicatie) te verkrijgen die is opgenomen in kredietverslagen, financiële bestanden en elektronische abonnee- en transactiebestanden ([290]). De wet inzake *national security letters* die toegang tot elektronische communicatie mogelijk maakt, mag alleen door de FBI worden gebruikt en vereist dat in de verzoeken een term wordt gebruikt die een persoon, entiteit, telefoonnummer of account specifiek identificeert en wordt bevestigd dat de informatie relevant is voor een geautoriseerd nationaal veiligheidsonderzoek ter bescherming tegen internationaal terrorisme of clandestiene inlichtingenactiviteiten ([291]). Ontvangers van een *national security letter* kunnen deze aanvechten in de rechtbank ([292]).

([281]) 50 U.S. Code § 1842, (c), (3) en, wat de *national security letters* betreft, 12 U.S.C. § 3414, (a), (2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v, (a); alsmede 18 U.S.C. § 2709(a).

([282]) Bij "een vertegenwoordiger van een buitenlandse mogendheid" kan het ook om niet-Amerikanen gaan die betrokken zijn bij internationaal terrorisme of de internationale verspreiding van massavernietigingswapens (inclusief voorbereidende handelingen) (50 U.S.C. § 1801 (b), (1)).

([283]) 50 U.S.C. § 1804. Zie ook § 1841, (4) met betrekking tot de keuze van de selectietermen.

([284]) 50 U.S.C. § 1821, (5).

([285]) 50 U.S.C. § 1823, (a).

([286]) 50 U.S.C. § 1842 in samenhang met § 1841(2) en sectie 3127 van titel 18.

([287]) 50 U.S.C. § 1862.

([288]) 50 U.S.C. §§ 1861-1862.

([289]) 50 U.S.C. § 1862(b).

([290]) 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; alsmede 18 U.S.C. § 2709.

([291]) 18 U.S.C. § 2709(b).

([292]) Bv. 18 U.S.C. § 2709(d).

3.2.1.3 *Verder gebruik van de verzamelde informatie*

(154) De verwerking van persoonsgegevens die door Amerikaanse inlichtingendiensten via SIGINT worden verzameld, is onderworpen aan een aantal waarborgen.

(155) Ten eerste moet elke inlichtingendienst zorgen voor passende gegevensbeveiliging en voorkomen dat onbevoegden toegang krijgen tot persoonsgegevens die via SIGINT zijn verzameld. In dit verband wordt in verschillende instrumenten, waaronder wetten, richtsnoeren en normen, nader bepaald aan welke minimumeisen inzake informatiebeveiliging moet worden voldaan (bv. multifactorauthenticatie, encryptie enz.) ([293]). De toegang tot de verzamelde gegevens moet worden beperkt tot bevoegd en opgeleid personeel dat de informatie nodig heeft om zijn taak uit te voeren ([294]). Meer in het algemeen moeten de inlichtingendiensten hun werknemers een passende opleiding geven, onder meer over de procedures voor het melden en aanpakken van schendingen van de wet (met inbegrip van EO 14086) ([295]).

(156) Ten tweede moeten de inlichtingendiensten voldoen aan de normen van de inlichtingendiensten inzake nauwkeurigheid en objectiviteit, met name wat betreft de kwaliteit en betrouwbaarheid van de gegevens, het in aanmerking nemen van alternatieve informatiebronnen en objectiviteit bij het uitvoeren van analyses ([296]).

(157) Ten derde verduidelijkt EO 14086 dat voor persoonsgegevens van niet-Amerikaanse personen dezelfde bewaartermijnen gelden als voor de gegevens van Amerikaanse personen ([297]). Inlichtingendiensten moeten specifieke bewaartermijnen vaststellen en/of de factoren definiëren waarmee rekening moet worden gehouden bij het vaststellen van de toepasselijke bewaartermijnen (bv. of de informatie bewijsmateriaal is voor een misdrijf; of de informatie uit buitenlandse inlichtingen bestaat; of de informatie noodzakelijk is om de veiligheid van personen of organisaties, met inbegrip van slachtoffers of doelwitten van internationaal terrorisme, te beschermen), die in verschillende rechtsinstrumenten zijn vastgelegd ([298]).

(158) Ten vierde gelden er specifieke regels voor de verspreiding van persoonsgegevens die via SIGINT zijn verzameld. Als algemene vereiste geldt dat persoonsgegevens over niet-Amerikaanse personen alleen mogen worden verspreid als het gaat om hetzelfde soort informatie dat over Amerikaanse personen mag worden verspreid, bijvoorbeeld informatie die nodig is om de veiligheid van een persoon of organisatie te beschermen (zoals doelwitten, slachtoffers of gijzelaars van internationale terroristische organisaties) ([299]). Bovendien mogen persoonsgegevens niet worden verspreid louter op grond van iemands nationaliteit of land van verblijf of om de vereisten van EO 14086 te omzeilen ([300]). Verspreiding binnen de Amerikaanse overheid mag alleen plaatsvinden indien een bevoegd en

([293]) Sectie 2, (c), (iii), (B), (1), EO 14086. Zie ook titel VIII van de National Security Act (waarin de vereisten voor toegang tot gerubriceerde informatie gedetailleerd worden beschreven), EO 12333, sectie 1.5 (op grond waarvan de hoofden van de instanties van de inlichtingendiensten zich moeten houden aan de richtsnoeren voor informatie-uitwisseling en -beveiliging, de privacy van informatie en andere wettelijke voorschriften), National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems" [Nationaal beleid voor de beveiliging van telecommunicatie- en informatiesystemen voor de nationale veiligheid] (op grond waarvan het Committee on National Security Systems richtsnoeren voor de beveiliging van nationale veiligheidssystemen moet verstrekken aan uitvoerende departementen en instanties), en National Security Memorandum 8, "Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems" [Verbetering van de cyberveiligheid van systemen van de nationale veiligheid, het ministerie van Defensie en de inlichtingendiensten] (met tijdschema's en richtsnoeren voor de uitvoering van cyberbeveiligingsvereisten voor nationale beveiligingssystemen, waaronder multifactorauthenticatie, encryptie, cloudtechnologieën en endpointdetectiediensten).

([294]) Sectie 2, (c), (iii), (B), (2), EO 14086. Bovendien zijn persoonsgegevens waarvoor geen definitieve vaststelling van bewaring is gedaan, alleen toegankelijk om een dergelijke vaststelling te doen of te ondersteunen of om toegestane administratieve, test-, ontwikkelings-, beveiligings- of toezichtfuncties uit te voeren (sectie 2, (c), (iii), (B), (3), EO 14086).

([295]) Sectie 2, (d), (ii), EO 14086.

([296]) Sectie 2, (c), (iii), (C), EO 14086.

([297]) Sectie 2, (c), (iii), (A), (2), (a)-(c), EO 14086. Meer in het algemeen moet elk agentschap beleid en procedures invoeren om de verspreiding en bewaring van via SIGINT verzamelde persoonsgegevens tot een minimum te beperken (sectie 2, (c), (iii), (A), EO 14086).

([298]) Zie bv. sectie 309 van de Intelligence Authorization Act For Fiscal Year 2015; minimaliseringsprocedures die door afzonderlijke inlichtingendiensten uit hoofde van sectie 702 FISA zijn vastgesteld en door de FISC zijn toegestaan; procedures die door de minister van Justitie en de FRA zijn goedgekeurd (en die de federale instanties van de VS, met inbegrip van de nationale veiligheidsdiensten, verplichten bewaartermijnen voor hun gegevens vast te stellen die door de National Archives and Record Administration moeten worden goedgekeurd).

([299]) Sectie 2, (c), (iii), (A), (1), (a) en sectie 5(d), EO 14086, in samenhang met sectie 2.3, EO 12333.

([300]) Sectie 2, (c), (iii), (A), (1), (b) en (e), EO 14086.

opgeleid persoon een redelijke overtuiging heeft dat de ontvanger de informatie nodig heeft ([301]) en deze naar behoren zal beschermen ([302]). Om te bepalen of persoonsgegevens mogen worden verspreid onder ontvangers buiten de Amerikaanse overheid (met inbegrip van een buitenlandse overheid of internationale organisatie), moet rekening worden gehouden met het doel van de verspreiding, de aard en de omvang van de verspreide gegevens en de mogelijke schadelijke gevolgen voor de betrokkene(n) ([303]).

(159) Ten slotte moet elke inlichtingendienst, mede om het toezicht op de naleving van de toepasselijke wettelijke voorschriften en de mogelijkheid van doeltreffende verhaalmechanismemogelijkheden te faciliteren, uit hoofde van EO 14086 passende documentatie over het verzamelen van SIGINT bijhouden. De documentatievereisten hebben betrekking op elementen zoals de feitelijke basis voor de beoordeling dat een specifieke verzamelingsactiviteit nodig is om een gevalideerde inlichtingenprioriteit te bevorderen ([304]).

(160) Naast de bovenvermelde waarborgen op grond van EO 14086 in verband met het gebruik van gegevens die met behulp van SIGINT zijn verzameld, gelden voor alle Amerikaanse inlichtingendiensten meer algemene voorschriften inzake doelbinding, minimale verwerking van gegevens, gegevensbeveiliging, nauwkeurigheid, bewaring en verspreiding van gegevens, die voortvloeien uit met name Circulaire nr. A-130 van het OMB, de E-Government Act, de Federal Records Act (zie overwegingen 101 - 106) en richtsnoeren van het Committee on National Security Systems (CNSS, comité nationale veiligheidssystemen) ([305]).

3.2.2 ***Toezicht***

(161) De activiteiten van de Amerikaanse inlichtingendiensten staan onder toezicht van verschillende instanties.

(162) Ten eerste vereist EO 14086 dat elke inlichtingendienst beschikt over hoge functionarissen op het gebied van wetgeving, toezicht en naleving om ervoor te zorgen dat de toepasselijke Amerikaanse wetgeving wordt nageleefd ([306]). Zij moeten met name periodiek toezicht houden op de SIGINT-activiteiten en ervoor zorgen dat alle gevallen van niet-naleving worden verholpen. De inlichtingendiensten moeten deze functionarissen toegang verlenen tot alle relevante informatie om hun toezichthoudende taken uit te voeren en mogen geen acties ondernemen om hun toezichthoudende activiteiten te belemmeren of op ongepaste wijze te beïnvloeden ([307]). Bovendien moet elk significant geval van niet-naleving ([308]) dat door een toezichthoudende functionaris of een andere werknemer wordt vastgesteld, onmiddellijk worden gemeld aan het hoofd van de inlichtingendienst en de Director of National Intelligence, die ervoor moet zorgen dat de nodige maatregelen worden genomen om het significante geval van niet-naleving te verhelpen en herhaling ervan te voorkomen ([309]).

(163) Deze toezichtfunctie wordt vervuld door functionarissen met een aangewezen nalevingsfunctie, alsmede door functionarissen voor privacy en burgerlijke vrijheden en inspecteurs-generaal ([310]).

([301]) De AGG-DOM, bijvoorbeeld, bepaalt dat de FBI uitsluitend informatie mag verspreiden indien de ontvanger van die informatie op de hoogte moet zijn om zijn opdracht tot een goed einde te brengen of om het publiek te beschermen.

([302]) Sectie 2, (c), (iii), (A), (1), (c), EO 14086. Inlichtingendiensten mogen bijvoorbeeld informatie verspreiden in omstandigheden die relevant zijn voor een strafrechtelijk onderzoek of in verband met een misdrijf, onder meer door bijvoorbeeld waarschuwingen te verspreiden in verband met dreigingen van moord, ernstig lichamelijk letsel of ontvoering; door informatie over cyberdreigingen, incidenten of reacties op onbevoegde toegang te verspreiden; en door slachtoffers op de hoogte te brengen of mogelijke slachtoffers van een misdrijf te waarschuwen.

([303]) Sectie 2, (c), (iii), (A), (1), (d), EO 14086.

([304]) Sectie 2, (c), (iii), (E), EO 14086.

([305]) Zie CNSS Policy No. 22, "Cybersecurity Risk Management Policy" [beleid inzake risicobeheer cyberbeveiliging] en CNSS Instruction 1253, waarin uitvoerige richtsnoeren worden verstrekt over veiligheidsmaatregelen die voor nationale veiligheidssystemen moeten worden ingevoerd.

([306]) Sectie 2, (d), (i), (A)-(B), EO 14086.

([307]) Sectie 2, (d), (i), (B)-(C), EO 14086.

([308]) D.w.z. een systematische of opzettelijke niet-naleving van de toepasselijke Amerikaanse wetgeving die de reputatie of integriteit van een onderdeel van de inlichtingendiensten zou kunnen aantasten of anderszins twijfel zou kunnen doen rijzen over de geoorloofdheid van een activiteit van de inlichtingendiensten, ook in het licht van belangrijke gevolgen voor de privacy en de burgerlijke vrijheden van de betrokken persoon of personen, zie sectie 5, (l), EO 14086.

([309]) Sectie 2, (d), (iii), EO 14086.

([310]) Sectie 2, (d), (i), (B), EO 14086.

(164) Net als bij de rechtshandhavingsinstanties zijn er bij alle inlichtingendiensten functionarissen voor privacy en burgerlijke vrijheden ([311]). De bevoegdheden van deze functionarissen omvatten doorgaans het toezicht op de procedures om ervoor te zorgen dat het/de respectieve ministerie/instantie op passende wijze rekening houdt met kwesties in verband met de privacy en de burgerlijke vrijheden, en passende procedures heeft ingevoerd voor de behandeling van klachten van natuurlijke personen die van mening zijn dat er inbreuk is gemaakt op hun privacy of burgerlijke vrijheden (en in sommige gevallen kunnen ze zelf de bevoegdheid hebben om klachten te onderzoeken, zoals het Office of the Director of National Intelligence (ODNI ([312]))). De hoofden van de inlichtingendiensten moeten ervoor zorgen dat de functionarissen voor privacy en burgerlijke vrijheden over de middelen beschikken om hun mandaat te vervullen, toegang krijgen tot al het materiaal en personeel dat nodig is om hun taken uit te voeren, en geïnformeerd en geraadpleegd worden over voorgestelde beleidswijzigingen ([313]). De functionarissen voor de burgerlijke vrijheden en de privacy brengen periodiek verslag uit aan het Congres en de PCLOB, onder meer over het aantal en de aard van de klachten die het ministerie/de instantie heeft ontvangen en het gevolg dat aan die klachten is gegeven, de uitgevoerde controles en onderzoeken en de gevolgen van de door de functionaris verrichte activiteiten ([314]).

(165) Ten tweede heeft elk onderdeel van de inlichtingendiensten een onafhankelijke inspecteur-generaal, die onder andere belast is met het toezicht op buitenlandse inlichtingenactiviteiten. Binnen het ODNI is dat het *Office of the Inspector General of the Intelligence Community* (bureau van de inspecteur-generaal van de inlichtingendiensten), dat uitgebreide rechtsmacht heeft over alle inlichtingendiensten en bevoegd is een onderzoek in te stellen naar klachten of informatie betreffende beschuldigingen van onrechtmatig gedrag of misbruik van gezag, in verband met programma's en activiteiten van het ODNI en/of de inlichtingendiensten ([315]). Zoals het geval is voor rechtshandhavingsinstanties (zie overweging 109), zijn deze inspecteurs-generaal wettelijk onafhankelijk ([316]) en zijn ze verantwoordelijk voor het uitvoeren van audits en onderzoeken met betrekking tot de door de betrokken dienst uitgevoerde programma's en operaties ten behoeve van nationaal inlichtingenwerk, onder meer wat misbruik of schending van de wet betreft ([317]). Zij hebben toegang tot alle gegevens, verslagen, audits, controles, documenten,

([311]) Zie 42 U.S.C. § 2000ee-1. Hiertoe behoren bijvoorbeeld het ministerie van Buitenlandse Zaken, het ministerie van Justitie, het ministerie van Binnenlandse Veiligheid, het ministerie van Defensie, de NSA, de Central Intelligence Agency (CIA, centrale inlichtingendienst), de FBI en het ODNI.

([312]) Zie sectie 3, (c), EO 14086.

([313]) 42 U.S.C. § 2000ee-1, (d).

([314]) Zie 42 U.S.C. § 2000ee-1, (f), (1) en (2). Uit het verslag van het Civil Liberties, Privacy and Transparency Office van de NSA voor de periode januari 2021 – juni 2021 blijkt bijvoorbeeld dat het 591 toetsingen heeft uitgevoerd naar de gevolgen voor de burgerlijke vrijheden en de privacy in verschillende contexten, bijvoorbeeld met betrekking tot verzamelactiviteiten, regelingen en besluiten inzake het delen van informatie, besluiten inzake het bewaren van gegevens enz., waarbij rekening werd gehouden met verschillende factoren, zoals de hoeveelheid en het soort informatie dat met de activiteit gepaard gaat, de betrokken natuurlijke personen, het doel en het verwachte gebruik van de gegevens, de bestaande waarborgen om mogelijke risico's voor de privacy te beperken enz. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Evenzo bevatten de verslagen van het Office of Privacy and Civil Liberties van de CIA voor de periode januari – juni 2019 informatie over de toezichtsactiviteiten van het bureau, bijvoorbeeld een toetsing van de naleving van de richtsnoeren van de minister van Justitie in het kader van EO 12333 met betrekking tot het bewaren en verspreiden van informatie, de verstrekte richtsnoeren over de uitvoering van PPD-28 en vereisten om gegevensinbreuken vast te stellen en aan te pakken, en beoordelingen van het gebruik en de behandeling van persoonlijke informatie (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf).

([315]) Deze inspecteur-generaal is benoemd door de president, met bevestiging van de Senaat, en kan alleen door de president worden ontslagen.

([316]) Inspecteurs-generaal zijn vast benoemd en kunnen alleen worden ontslagen door de president, die het Congres schriftelijk op de hoogte moet brengen van de redenen voor een dergelijk ontslag. Dit houdt niet noodzakelijkerwijs in dat zij geheel vrij van instructies zijn. In sommige gevallen kan het hoofd van het ministerie de inspecteur-generaal verbieden om een audit of onderzoek te starten, uit te voeren of af te ronden als dat noodzakelijk wordt geacht om belangrijke nationale (veiligheids)belangen te vrijwaren. Het Congres moet echter op de hoogte worden gebracht van de uitoefening van die bevoegdheid en kan op grond daarvan de verantwoordelijkheid bij de betrokken directeur leggen. Zie bv. Inspector General Act of 1978, § 8 (voor het ministerie van Defensie); § 8E (voor het ministerie van Justitie), § 8G, (d), (2), (A) en (B) (voor de NSA); 50. U.S.C. § 403q, (b) (voor de CIA); Intelligence Authorization Act For Fiscal Year 2010, sectie 405(f) (voor de inlichtingendiensten).

([317]) Inspector General Act of 1978, zoals gewijzigd, Pub. L. 117-108 van 8 april 2022. Zo heeft de inspecteur-generaal van de NSA, zoals uiteengezet in zijn halfjaarlijkse verslagen aan het Congres over de periode van 1 april 2021 tot en met 31 maart 2022, toetsingen verricht van de behandeling van op grond van EO 12333 verzamelde informatie over Amerikaanse personen, het proces voor het zuiveren van SIGINT-gegevens, een door de NSA gebruikt geautomatiseerd instrument voor het specificeren van doelwitten, en de naleving van de documentatie- en doorzoekingsregels met betrekking tot het verzamelen op grond van sectie 702 FISA, en in dit verband verscheidene aanbevelingen gedaan (zie https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, blz. 5-8 en https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907, blz. 10-13). Zie ook de recente audits en onderzoeken van de inspecteur-generaal van de inlichtingendiensten naar informatiebeveiliging en ongeoorloofde openbaarmaking van gerubriceerde nationale veiligheidsinformatie (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, blz. 8 en 11 en https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct 2021-Mar 2022 ICIG SAR_Unclass_FINAL.pdf, blz. 19-20).

papieren, aanbevelingen en ander relevant materiaal, zo nodig door een dwangbevel, en kunnen getuigenverklaringen afnemen ([318]). De inspecteurs-generaal verwijzen gevallen van vermoedelijke strafbare feiten voor vervolging door en doen aanbevelingen voor corrigerende maatregelen aan de hoofden van de diensten ([319]). Hoewel hun aanbevelingen niet bindend zijn, worden hun verslagen, met inbegrip van de follow-up (of het ontbreken daarvan) ([320]) in het algemeen openbaar gemaakt en toegezonden aan het Congres, dat op basis daarvan zijn eigen toezichtfunctie kan uitoefenen (zie overwegingen 168-169) ([321]).

(166) Ten slotte houdt de *Intelligence Oversight Board* (toezichtsraad inzake inlichtingen, hierna "IOB"), die is opgericht binnen de *President's Intelligence Advisory Board* (adviesraad van de president inzake inlichtingen, hierna "PIAB"), toezicht op de naleving van de grondwet en alle geldende regels door de Amerikaanse inlichtingendiensten ([322]). De PIAB is een adviesorgaan binnen het *Executive Office* van de president dat bestaat uit 16 door de president benoemde leden van buiten de Amerikaanse overheid. De IOB bestaat uit ten hoogste vijf leden die door de president worden aangewezen uit de leden van de PIAB. Volgens EO 12333 ([323]) zijn de hoofden van alle inlichtingendiensten verplicht bij de IOB melding te maken van elke inlichtingenactiviteit waarbij er reden is om aan te nemen dat deze onwettig is of in strijd met een Executive Order of een Presidential Directive. Om ervoor te zorgen dat de IOB toegang heeft tot de informatie die hij nodig heeft om zijn functies uit te oefenen, draagt Executive Order 13462 de Director of National Intelligence en de hoofden van de inlichtingendiensten op alle informatie en bijstand te verstrekken die de IOB nodig acht om zijn functies uit te oefenen, voor zover de wet dat toestaat ([324]). De IOB moet op zijn beurt de president informeren over inlichtingenactiviteiten die naar zijn mening in strijd zijn met de Amerikaanse wetgeving (met inbegrip van Executive Orders) en die niet adequaat worden aangepakt door de minister van Justitie, de Director of National Intelligence of het hoofd van een inlichtingendienst ([325]). Bovendien moet de IOB de minister van Justitie informeren over mogelijke schendingen van het strafrecht.

(167) Ten vierde staan de inlichtingendiensten onder toezicht van de PCLOB. Volgens het oprichtingsstatuut is de PCLOB belast met verantwoordelijkheden op het gebied van terrorismebestrijding en de uitvoering daarvan, met het oog op de bescherming van de privacy en de burgerlijke vrijheden. Voor haar controle van het optreden van de inlichtingendiensten heeft deze instantie toegang tot alle relevante gegevens, verslagen, audits, controles, documenten, papieren en aanbevelingen van de diensten, inclusief gerubriceerde informatie, en kan zij gesprekken voeren en getuigen oproepen ([326]). Zij ontvangt de verslagen van de functionarissen voor de burgerlijke vrijheden en de privacy van verschillende federale ministeries/instanties ([327]), kan aanbevelingen doen aan de overheid en de inlichtingendiensten en brengt regelmatig verslag uit aan de Committees (commissies) van het Congres en de president ([328]). Verslagen van de PCLOB, ook die aan het Congres, moeten zoveel mogelijk openbaar worden gemaakt ([329]). De PCLOB heeft verscheidene toezicht- en follow-upverslagen uitgebracht, waaronder een analyse van de programma's die op basis van sectie 702 FISA worden uitgevoerd en de bescherming van de privacy in deze context, de uitvoering van PPD-28 en EO 12333 ([330]). De PCLOB is ook belast met het uitvoeren van specifieke toezichtfuncties met betrekking

([318]) Zie de Inspector General Act van 1978, § 6.

([319]) Zie de Inspector General Act van 1978, §§ 4 en 6-5.

([320]) Wat betreft de follow-up die wordt gegeven aan verslagen en aanbevelingen van inspecteurs-generaal, zie bv. de reactie op een verslag van de inspecteur-generaal van het ministerie van Justitie waarin werd vastgesteld dat de FBI niet voldoende transparant was met de FISC in aanvragen van 2014 tot 2019, hetgeen leidde tot hervormingen om de naleving, het toezicht en de verantwoordingsplicht bij de FBI te verbeteren (zo gaf de directeur van de FBI opdracht tot meer dan 40 corrigerende maatregelen, waaronder 12 specifiek voor het FISA-proces met betrekking tot documentatie, toezicht, het bijhouden van dossiers, opleiding en audits) (zie https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance en https://oig.justice.gov/reports/2019/o20012.pdf). Zie bijvoorbeeld ook de audit van de inspecteur-generaal van het ministerie van Justitie over de rol en de verantwoordelijkheden van het *Office of the General Counsel* (bureau voor juridisch advies) van de FBI bij het toezicht op de naleving van de toepasselijke wetten, beleidsmaatregelen en procedures in verband met de nationale veiligheidsactiviteiten van de FBI en bijlage 2, die een brief van de FBI bevat waarin alle aanbevelingen worden aanvaard. In dit verband geeft bijlage 3 een overzicht van de vervolgmaatregelen en informatie die de inspecteur-generaal van de FBI verlangde om zijn aanbevelingen te kunnen afsluiten (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

([321]) Zie de Inspector General Act van 1978, § 4(5) en § 5.

([322]) Zie EO 13462.

([323]) Sectie 1.6, (c), EO 12333.

([324]) Sectie 8, (a), EO 13462.

([325]) Sectie 6, (b), EO 13462.

([326]) 42 U.S.C. § 2000ee, (g).

([327]) Zie 42 U.S.C. § 2000ee-1, (f), (1), (A), (iii). Hiertoe behoren ten minste het ministerie van Justitie, het ministerie van Defensie, het ministerie van Binnenlandse Veiligheid, de Director of National Intelligence en de CIA, plus eventuele andere ministeries, diensten of onderdelen van de uitvoerende macht waarvoor de Privacy and Civil Liberties Oversight Board verslaggeving passend acht.

([328]) 42 U.S.C. § 2000ee (e).

([329]) 42 U.S.C. § 2000ee, (f).

([330]) Beschikbaar op https://www.pclob.gov/Oversight

tot de uitvoering van EO 14086, met name door na te gaan of de procedures van de instanties in overeenstemming zijn met het EO (zie overweging 126) en door de werking van het verhaalmechanisme te evalueren (zie overweging 194).

(168) Ten vijfde hebben specifieke commissies (Committees) in het Amerikaanse Congres (met name de Intelligence and Judiciary Committees (Commissies inlichtingen en Commissies juridische zaken) van het Huis van Afgevaardigden en de Senaat), naast deze toezichtsmechanismen binnen de uitvoerende macht, verantwoordelijkheden voor het toezicht op alle buitenlandse inlichtingenactiviteiten van de Verenigde Staten. De leden van deze commissies hebben toegang tot gerubriceerde informatie en inlichtingenmethoden en -programma's ([331]). De commissies oefenen hun toezichtfuncties op verschillende manieren uit, met name via hoorzittingen, onderzoeken, evaluaties en verslagen ([332]).

(169) De commissies van het Congres ontvangen regelmatig verslagen over inlichtingenactiviteiten, onder meer van de minister van Justitie, de Director of National Intelligence, de inlichtingendiensten en andere toezichthoudende instanties (bv. inspecteurs-generaal), zie de overwegingen 164-165. De National Security Act bepaalt met name dat de president ervoor moet zorgen dat de Intelligence Committees van het Congres ten volle en actueel op de hoogte worden gehouden van de inlichtingenactiviteiten van de Verenigde Staten, met inbegrip van alle belangrijke verwachte inlichtingenactiviteiten in de zin van dit subhoofdstuk ([333]). Bovendien zorgt de president ervoor dat alle illegale inlichtingenactiviteiten onmiddellijk aan de Intelligence Committees van het Congres worden gemeld, evenals de corrigerende maatregelen die zijn genomen of worden gepland in verband met deze illegale activiteiten ([334]).

(170) Bovendien vloeien uit specifieke wetten aanvullende rapportageverplichtingen voort. In het bijzonder schrijft de FISA voor dat de minister van Justitie de Intelligence and Judiciary Committees (Commissies inlichtingen en Commissies juridische zaken) van het Huis van Afgevaardigden en de Senaat "ten volle moet informeren" over de activiteiten van de overheid in het kader van bepaalde secties van de FISA ([335]). De FISA schrijft ook voor dat de overheid de commissies van het Congres moet voorzien van afschriften van alle beslissingen, bevelen of adviezen van de FISC of de FISCR die een "essentiële uitlegging of interpretatie" bevatten van bepalingen van de FISA. Met betrekking tot surveillance op grond van sectie 702 FISA wordt het parlementaire toezicht uitgeoefend door middel van wettelijk verplichte verslagen aan de Intelligence and Judiciary Committees en frequente briefings en hoorzittingen. Die verslagen omvatten een halfjaarlijks verslag van de minister van Justitie waarin de toepassing van sectie 702 FISA wordt beschreven, met bewijsstukken waaronder met name de nalevingsverslagen van het ministerie van Justitie en het ODNI en een beschrijving van eventuele gevallen van niet-naleving ([336]), en een afzonderlijke halfjaarlijkse beoordeling van de minister van Justitie en de Director of National Intelligence waarin de naleving van de procedures om het doelwit te specificeren en de minimaliseringsprocedures wordt gedocumenteerd ([337]).

([331]) 50 U.S.C. § 3091.

([332]) Zo organiseren de commissies thematische hoorzittingen (zie bijvoorbeeld een recente hoorzitting van de House Judiciary Committee over "digital dragnets", https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983, en een hoorzitting van de House Intelligence Committee over het gebruik van AI door de inlichtingendiensten, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263) alsook regelmatige toezichtshoorzittingen, bijvoorbeeld van de nationale veiligheidsdivisie van de FBI en het ministerie van Justitie, zie https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 en https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899. Zie als voorbeeld van een onderzoek het onderzoek van de Senate Intelligence Committee naar Russische inmenging in de Amerikaanse verkiezingen van 2016, zie https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures. Zie qua rapportage bijvoorbeeld het overzicht van de (toezichts)activiteiten van de commissie in het verslag van de Senate Intelligence Committee over de periode 4 januari 2019 – 3 januari 2021 aan de Senaat, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4

([333]) Zie 50 U.S.C. § 3091, (a), (1). Deze bepaling bevat de algemene vereisten met betrekking tot het toezicht van het Congres op het gebied van de nationale veiligheid.

([334]) Zie 50 U.S.C. § 3091, (b).

([335]) Zie 50 U.S.C. §§ 1808, 1846, 1862, 1871 en 1881f.

([336]) Zie 50 U.S.C. § 1881f.

([337]) Zie 50 U.S.C. § 1881a, (l), (1).

(171) Overeenkomstig de FISA moet de Amerikaanse overheid bovendien elk jaar aan het Congres (en het publiek) onder andere het aantal gevraagde en ontvangen FISA-bevelen bekendmaken, evenals ramingen van het aantal Amerikanen en niet-Amerikanen die het doelwit van surveillance zijn ([338]). De USA Freedom Act vereist ook aanvullende openbare verslaggeving over het aantal afgegeven *national security letters*, opnieuw zowel met betrekking tot Amerikanen als niet-Amerikanen (en biedt de ontvangers van FISA-bevelen en certificeringen, alsook van verzoeken op basis van *national security letters*, tegelijkertijd de mogelijkheid om onder bepaalde voorwaarden transparantieverslagen op te stellen) ([339]).

(172) Meer in het algemeen ondernemen de Amerikaanse inlichtingendiensten verschillende inspanningen om transparantie te verschaffen over hun (buitenlandse) inlichtingenactiviteiten. Zo heeft het ODNI in 2015 beginselen voor transparantie van inlichtingen en een uitvoeringsplan voor transparantie aangenomen en elke inlichtingendienst opgedragen een functionaris voor transparantie van inlichtingen aan te wijzen om transparantie te bevorderen en initiatieven voor transparantie te leiden ([340]). Als onderdeel van deze inspanningen hebben de inlichtingendiensten delen van beleid, procedures, toezichtsverslagen, verslagen over activiteiten in het kader van sectie 702 FISA en EO 12333, besluiten van de FISC en ander materiaal gederubriceerd en blijven zij dit doen, onder meer op een speciale webpagina "IC on the Record", beheerd door het ODNI ([341]).

(173) Ten slotte is het verzamelen van persoonsgegevens uit hoofde van sectie 702 FISA, naast het toezicht door de in de overwegingen 162 tot en met 168 genoemde toezichthoudende instanties, onderworpen aan het toezicht van de FISC ([342]). Krachtens regel 13 van het reglement van orde van de FISC moeten de compliance officers van de Amerikaanse inlichtingendiensten alle schendingen van de procedures om het doelwit te specificeren, minimaliseringsprocedures en procedures voor het doorzoeken uit hoofde van sectie 702 FISA melden aan het ministerie van Justitie en het ODNI, die ze op hun beurt melden aan de FISC. Bovendien dienen het ministerie van Justitie en het ODNI halfjaarlijkse gezamenlijke verslagen over het toezicht in bij de FISC, waarin trends in de naleving van de doelstellingen worden vastgesteld; statistische gegevens worden verstrekt; categorieën nalevingsincidenten worden beschreven; in detail wordt beschreven waarom bepaalde incidenten in verband met de naleving van het specificeren van doelwitten hebben plaatsgevonden en wordt aangegeven welke maatregelen de inlichtingendiensten hebben genomen om herhaling te voorkomen ([343]).

(174) Indien nodig (bv. indien schendingen van de procedures voor het specificeren van doelwitten worden vastgesteld), kan de FISC de betrokken inlichtingendienst gelasten corrigerende maatregelen te nemen ([344]). Hierbij kan het gaan om individuele en structurele maatregelen, zoals het beëindigen van de gegevensverwerving en het wissen van onrechtmatig verkregen gegevens, tot een verandering in de praktijk van het verzamelen, maar ook richtsnoeren voor en opleiding van personeel ([345]). Bovendien bekijkt de FISC bij zijn jaarlijkse toetsing van de certificeringen uit hoofde van sectie 702 naar de gevallen van niet-naleving om te bepalen of de ingediende certificeringen voldoen

([338]) 50 U.S.C. § 1873(b). Bovendien voert de Director of National Intelligence overeenkomstig sectie 402 in overleg met de minister van Justitie een beoordeling uit inzake de derubricering van alle door de Foreign Intelligence Surveillance Court of de Foreign Intelligence Surveillance Court of Review (zoals gedefinieerd in sectie 601(e)) uitgevaardigde beslissingen, bevelen en adviezen die een essentiële uitlegging of interpretatie van een wettelijke bepaling bevatten, inclusief elke nieuwe of essentiële uitlegging of interpretatie van het begrip "specifieke selectieterm", en maakt deze beslissingen, bevelen en adviezen overeenkomstig die beoordeling voor zover praktisch mogelijk voor het publiek toegankelijk.

([339]) 50 U.S.C. §§ 1873, (b), (7) en 1874.

([340]) https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic

([341]) Zie "IC on the Record", beschikbaar op https://icontherecord.tumblr.com/

([342]) In het verleden concludeerde de FISC dat het voor de rechtbank duidelijk is dat de uitvoerende instanties, evenals [het ODNI] en [de National Security Division van het ministerie van Justitie], aanzienlijke middelen besteden aan hun verantwoordelijkheden inzake naleving en toezicht op grond van sectie 702. Als algemene regel geldt dat gevallen van niet-naleving onmiddellijk worden vastgesteld en dat passende corrigerende maatregelen worden genomen, waaronder het wissen van informatie die ten onrechte is verkregen of waarvoor anderszins krachtens de toepasselijke procedures vernietigingsvoorschriften gelden. FISA Court, "Memorandum Opinion and Order" [titel gerubriceerd] (2014), beschikbaar op https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf

([343]) Zie bv. "FISA 702 Compliance Report" [FISA 702-nalevingsverslag] van het ministerie van Justitie/ODNI aan de FISC voor de periode juni 2018 – november 2018, blz. 21-65.

([344]) 50 U.S.C. § 1803, (h). Zie ook PCLOB, "Section 702 Report" (Verslag over sectie 702), blz. 76. Zie voorts het "Memorandum Opinion and Order" van de FISC van 3 oktober 2011 als voorbeeld van een *deficiency order* waarin de overheid werd gelast de vastgestelde tekortkomingen binnen 30 dagen te verhelpen. Beschikbaar op https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and Order-20140716.pdf. Zie Walton-brief, sectie 4, blz. 10-11. Zie ook het advies van de FISC van 18 oktober 2018, beschikbaar op https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, zoals bevestigd door de Foreign Intelligence Court of Review in zijn advies van 12 juli 2019, beschikbaar op https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, waarin de FISC de overheid onder meer gelastte te voldoen aan bepaalde meldings-, documentatie- en rapportageverplichtingen jegens de FISC.

([345]) Zie bv. het "Memorandum Opinion and Order" van de FISC, blz. 76 (6 december 2019) (goedgekeurd voor openbare bekendmaking op 4 september 2020), waarin de FISC de overheid opdroeg uiterlijk 28 februari 2020 een schriftelijk verslag in te dienen over de stappen die de overheid ondernam ter verbetering van de processen voor het identificeren en verwijderen van verslagen die zijn afgeleid van FISA 702-informatie en die om nalevingsredenen zijn teruggeroepen, alsmede over andere aangelegenheden. Zie ook bijlage VII.

aan de vereisten van de FISA. Evenzo kan de FISC, indien hij van oordeel is dat de certificeringen van de overheid ontoereikend waren, onder meer wegens bepaalde gevallen van niet-naleving, een zogenaamd *deficiency order* (nalatigheidsbevel) uitvaardigen waarin de overheid wordt gelast de schending binnen 30 dagen te verhelpen of waarin de overheid wordt gelast de uitvoering van de certificering uit hoofde van sectie 702 te staken of er niet mee te beginnen. Ten slotte beoordeelt de FISC trends die hij waarneemt in nalevingskwesties en kan hij wijzigingen in procedures of aanvullend toezicht en rapportage verlangen om nalevingstrends aan te pakken ([346]).

3.2.3 ***Verhaalmechanismemogelijkheden***

(175) Zoals in deze sectie nader wordt toegelicht, biedt een aantal rechtsmiddelen in de Verenigde Staten betrokkenen uit de Unie de mogelijkheid een rechtszaak aan te spannen voor een onafhankelijk en onpartijdig gerecht met bindende bevoegdheden. Samen stellen zij natuurlijke personen in staat toegang te krijgen tot hun persoonsgegevens, de rechtmatigheid van de toegang van de overheid tot hun gegevens te laten toetsen en, indien een schending wordt vastgesteld, die schending ongedaan te laten maken, onder meer door rectificatie of wissing van hun persoonsgegevens.

(176) Ten eerste wordt bij EO 14086, aangevuld met de AG Regulation tot oprichting van de Data Protection Review Court, een specifiek verhaalmechanisme ingesteld om klachten van natuurlijke personen over Amerikaanse SIGINT-activiteiten te behandelen en op te lossen. Elke natuurlijke persoon in de EU heeft het recht bij het verhaalmechanisme een klacht in te dienen over een vermeende schending van de Amerikaanse wetgeving inzake SIGINT-activiteiten (bv. EO 14086, sectie 702 FISA, EO 12333) die zijn belangen inzake privacy en burgerlijke vrijheden schaadt ([347]). Dit verhaalmechanisme staat open voor personen uit landen of regionale organisaties voor economische integratie die door de minister van Justitie van de VS zijn aangewezen als "in aanmerking komende staten" ([348]). Op 30 juni 2023 zijn de Europese Unie en de drie landen van de Europese Vrijhandelsassociatie die samen de Europese Economische Ruimte vormen door de minister van Justitie overeenkomstig sectie 3,(f), van de EO 14086 aangewezen als "in aanmerking komende staten" ([349]). Deze aanwijzing doet geen afbreuk aan artikel 4, lid 2, van het Verdrag betreffende de Europese Unie.

(177) Een betrokkene uit de Unie die een dergelijke klacht wil indienen, moet deze indienen bij een toezichthoudende autoriteit in een EU-lidstaat die bevoegd is voor het toezicht op de verwerking van persoonsgegevens door overheidsdiensten (een gegevensbeschermingsautoriteit) ([350]). Dit zorgt voor een gemakkelijke toegang tot het verhaalmechanisme doordat personen zich kunnen wenden tot een instantie "dicht bij huis" en waarmee zij in hun eigen taal kunnen communiceren. Na verificatie van de in overweging 178 bedoelde vereisten voor de indiening van een klacht zal de bevoegde gegevensbeschermingsautoriteit de klacht via het secretariaat van het Europees Comité voor gegevensbescherming doorsturen naar het verhaalmechanisme

(178) Voor het indienen van een klacht bij het verhaalmechanisme gelden lage ontvankelijkheidsvereisten, aangezien natuurlijke personen niet hoeven aan te tonen dat hun gegevens daadwerkelijk het voorwerp zijn geweest van Amerikaanse SIGINT-activiteiten ([351]). Om het verhaalmechanisme in staat te stellen een toetsing uit te voeren, moet tegelijkertijd bepaalde basisinformatie worden verstrekt, bijvoorbeeld over de persoonsgegevens waarvan redelijkerwijs mag worden aangenomen dat zij naar de VS zijn doorgegeven en de wijze waarop dat is gebeurd; de identiteit van de entiteiten van de Amerikaanse overheid die vermoedelijk bij de vermeende schending betrokken zijn (indien bekend); de grondslag voor de bewering dat een schending van het Amerikaanse recht heeft plaatsgevonden (hoewel ook hier niet hoeft te worden aangetoond dat de persoonsgegevens daadwerkelijk door de Amerikaanse inlichtingendiensten zijn verzameld) en de aard van het gevorderde redres.

([346]) Zie bijlage VII.

([347]) Zie sectie 4, (k), (iv), EO 14086, die bepaalt dat een klacht bij het verhaalmechanisme moet worden ingediend door een klager die namens zichzelf optreedt (d.w.z. niet als vertegenwoordiger van een regering, niet-gouvernementele of intergouvernementele organisatie). Het begrip "benadeeld zijn" vereist niet dat de klager aan een bepaalde drempel moet voldoen om toegang te krijgen tot het verhaalmechanisme (zie hierover overweging 178). Het verduidelijkt wel dat de CLPO van het ODNI en de DPRC bevoegd zijn om inbreuken op het Amerikaanse recht in verband met SIGINT-activiteiten die de individuele privacy van een klager en diens burgerlijke vrijheden benadelen te verhelpen. Inbreuken op voorschriften uit hoofde van toepasselijk Amerikaans recht die niet bedoeld zijn om natuurlijke personen te beschermen (bv. budgettaire voorschriften), zouden daarentegen niet onder de rechtsbevoegdheid van de CLPO van het ODNI en de DPRC vallen.

([348]) Sectie 3, (f), EO 14086.

([349]) https://www.justice.gov/opcl/executive-order-14086.

([350]) Sectie 4, (d), (v), EO 14086.

([351]) Zie sectie 4(k)(i)-(iv) EO 14086.

(179) Het initiële onderzoek van klachten bij dit verhaalmechanisme wordt uitgevoerd door de CLPO van het ODNI, wiens bestaande wettelijke rol en bevoegdheden zijn uitgebreid voor die specifieke acties die worden ondernomen overeenkomstig EO 14086 ([352]). Binnen de inlichtingendiensten is de CLPO er onder meer verantwoordelijk voor dat de bescherming van de burgerlijke vrijheden en de privacy op passende wijze wordt opgenomen in het beleid en de procedures van het ODNI en de inlichtingendiensten; ziet hij toe op de naleving door het ODNI van de toepasselijke voorschriften inzake burgerlijke vrijheden en privacy; en voert hij privacy-effectbeoordelingen uit ([353]). De CLPO van het ODNI kan alleen door de Director of National Intelligence worden ontslagen om gegronde redenen, d.w.z. in geval van wangedrag, ambtsmisdrijf, inbreuk op de veiligheid, plichtsverzuim of onbekwaamheid ([354]).

(180) Bij het uitvoeren van zijn beoordeling heeft de CLPO van het ODNI toegang tot de informatie voor zijn beoordeling en kan hij rekenen op de gedwongen bijstand van functionarissen voor privacy en burgerlijke vrijheden binnen de verschillende inlichtingendiensten ([355]). Het is de inlichtingendiensten verboden de beoordelingen van de CLPO van het ODNI te belemmeren of op ongepaste wijze te beïnvloeden. Dit geldt ook voor de Director of National Intelligence, die zich niet met de evaluatie mag bemoeien ([356]). Bij de beoordeling van een klacht moet de CLPO van het ODNI de wet "onpartijdig toepassen", met inachtneming van zowel de nationale veiligheidsbelangen bij SIGINT-activiteiten als de bescherming van de privacy ([357]).

(181) Als onderdeel van zijn onderzoek bepaalt de CLPO van het ODNI of er sprake is van een schending van de toepasselijke Amerikaanse wetgeving en, indien dat het geval is, beslist hij over passende herstelmaatregelen ([358]). Dit laatste betreft maatregelen die een vastgestelde schending volledig ongedaan maken, zoals beëindiging van de onrechtmatige verkrijging van gegevens, wissing van onrechtmatig verzamelde gegevens, wissing van de resultaten van onrechtmatig verrichte bevragingen van overigens rechtmatig verzamelde gegevens, beperking van de toegang tot rechtmatig verzamelde gegevens tot naar behoren opgeleid personeel, of het terugroepen van inlichtingen-rapporten die gegevens bevatten die zonder rechtmatige toestemming zijn verkregen of die onrechtmatig zijn verspreid ([359]). Beslissingen van de CLPO van het ODNI over individuele klachten (inclusief over de herstelmaatregelen) zijn bindend voor de betrokken inlichtingendiensten ([360]).

(182) De CLPO van het ODNI moet de documentatie van zijn onderzoek bijhouden en een gerubriceerd besluit opstellen waarin de grondslag voor zijn feitelijke bevindingen wordt toegelicht, alsmede de vaststelling of er sprake is van een onder EO 14086 vallende schending en de vaststelling van passende herstelmaatregelen ([361]). Indien uit het onderzoek van de CLPO van het ODNI een schending blijkt van een autoriteit waarop de FISC toezicht houdt, moet de CLPO ook een gerubriceerd verslag indienen bij de adjunct-minister van Justitie voor nationale veiligheid (*Assistant Attorney General for National Security*), die op zijn beurt verplicht is de niet-naleving te melden aan de FISC, die verdere handhavingsmaatregelen kan nemen (overeenkomstig de in de overwegingen 173-174 beschreven procedure) ([362]).

(183) 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 dat de CLPO van het ODNI een besluit heeft genomen dat passende herstelmaatregelen vereist ([363]). Hierdoor kan de vertrouwelijkheid van activiteiten ter bescherming van de nationale veiligheid worden beschermd, terwijl de betrokkenen een besluit krijgen dat bevestigt dat hun klacht naar behoren is onderzocht en beoordeeld. Dit besluit kan bovendien door de natuurlijke persoon worden aangevochten. Daartoe zal hij worden geïnformeerd over de mogelijkheid om bij de DPRC in beroep te gaan tegen de vaststellingen van de CLPO (zie de overwegingen 184 en verder) en dat, ingeval de zaak bij de rechtbank aanhangig zou worden gemaakt, een bijzondere jurist (*special advocate*) zal worden gekozen om de belangen van de klager te behartigen ([364]).

([352]) Sectie 3, (c), (iv), EO 14086. Zie ook National Security Act 1947, 50 U.S.C. §403-3d, sectie 103D, betreffende de rol van de CLPO binnen het ODNI.
([353]) 50 U.S.C § 3029 (b).
([354]) Sectie 3, (c), (iv), EO 14086.
([355]) Sectie 3, (c), (iii), EO 14086.
([356]) Sectie 3, (c), (iv), EO 14086.
([357]) Sectie 3, (c), (i), (B), (i) en (iii), EO 14086.
([358]) Sectie 3, (c), (i), EO 14086.
([359]) Sectie 4, (a), EO 14086.
([360]) Sectie 3, (c), (d), EO 14086.
([361]) Sectie 3, (c), (i), (F)-(G), EO 14086.
([362]) Zie ook sectie 3, (c), (i), (D), EO 14086.
([363]) Sectie 3, (c), (i), (E), (1), EO 14086.
([364]) Sectie 3, (c), (i), (E), (2)-(3), EO 14086.

(184) Elke klager en elk onderdeel van de inlichtingendiensten kan de beslissing van de CLPO van het ODNI laten toetsen door de Data Protection Review Court (DPRC). Dergelijke verzoeken om toetsing moeten worden ingediend binnen 60 dagen na ontvangst van de kennisgeving van de CLPO van het ODNI dat zijn toetsing is voltooid en moeten alle informatie bevatten die de betrokkene aan de DPRC wenst te verstrekken (bv. argumenten inzake rechtsvragen of de toepassing van het recht op de feiten van de zaak) ([365]). De betrokkenen in de Unie kunnen hun aanvraag opnieuw via de bevoegde gegevensbeschermingsautoriteit (zie overweging 177).

(185) De DPRC is een onafhankelijke rechterlijke instantie die door de minister van Justitie is ingesteld op grond van EO 14086 ([366]). Hij bestaat uit ten minste zes rechters, die door de minister van Justitie in overleg met de PCLOB, de minister van Handel en de Director of National Intelligence worden benoemd voor hernieuwbare termijnen van vier jaar ([367]). De benoeming van rechters door de minister van Justitie is gebaseerd op de criteria die de uitvoerende macht hanteert bij de beoordeling van kandidaten voor de federale rechterlijke macht, waarbij belang wordt gehecht aan eerdere justitiële ervaring ([368]). Bovendien moeten de rechters beoefenaars van juridische beroepen zijn (d.w.z. actieve leden met een goede reputatie bij de balie en naar behoren gemachtigd voor de advocatuur) en passende ervaring hebben op het gebied van privacy en nationale veiligheidswetgeving. De minister van Justitie moet ernaar streven dat ten minste de helft van de rechters op enig moment eerdere justitiële ervaring heeft en alle rechters moeten over een veiligheidsmachtiging beschikken om toegang te kunnen krijgen tot gerubriceerde nationale veiligheidsinformatie ([369]).

(186) Alleen personen die voldoen aan de in overweging 185 genoemde kwalificaties en die op het tijdstip van hun benoeming of in de twee voorafgaande jaren geen werknemer van de uitvoerende macht zijn, kunnen tot lid van de DPRC worden benoemd. Evenzo mogen de rechters tijdens hun ambtstermijn bij de DPRC geen officiële taken of banen binnen de Amerikaanse regering hebben (anders dan als rechter bij de DPRC) ([370]).

(187) De onafhankelijkheid van het berechtingsproces wordt bereikt door een aantal garanties. Met name is het de uitvoerende macht (de minister van Justitie en de inlichtingendiensten) verboden zich te mengen in de evaluatie van de DPRC of deze op ongepaste wijze te beïnvloeden ([371]). De DPRC zelf moet onpartijdig uitspraak doen in zaken ([372]) en werkt volgens zijn eigen reglement van orde (aangenomen bij meerderheid van stemmen). Bovendien kunnen rechters van de DPRC uitsluitend om gegronde redenen (d.w.z. wangedrag, ambtsmisdrijf, inbreuk op de veiligheid, plichtsverzuim of onbekwaamheid) en uitsluitend door de minister van Justitie worden ontslagen, nadat naar behoren rekening is gehouden met de normen voor federale rechters die zijn neergelegd in de "Rules for Judicial-Conduct and Judicial-Disability Proceedings" (regels voor het gedrag van rechters en voor procedures inzake onbekwaamheid van rechters) ([373]).

([365]) Sectie 201.6, (a)-(b), AG Regulation.

([366]) Sectie 3, (d), (i) en de AG Regulation. Het Hooggerechtshof van de Verenigde Staten heeft de mogelijkheid voor de minister van Justitie erkend om onafhankelijke organen met beslissingsbevoegdheid op te richten, ook om individuele zaken te berechten, zie met name United States ex rel. Accardi/Shaughnessy, 347 U.S. 260 (1954) en United States/Nixon, 418 U.S. 683, 695 (1974). Op de naleving van de verschillende voorschriften van EO 14086, bv. de criteria en procedure voor de aanstelling en het ontslag van rechters van de DPRC, wordt met name toegezien door de inspecteur-generaal van het ministerie van Justitie (zie ook overweging 109 over de wettelijke bevoegdheid van inspecteurs-generaal).

([367]) Sectie 3, (d), (i), (A), EO 14086 en sectie 201.3, (a), AG Regulation.

([368]) Sectie 201.3, (b), AG Regulation.

([369]) Sectie 3, (d), (i), (B), EO 14086.

([370]) Sectie 3, (d), (i), (A), EO 14086 en sectie 201.3, (a) en (c), AG Regulation. In het DPRC benoemde personen mogen deelnemen aan buitengerechtelijke activiteiten, waaronder zakelijke en financiële activiteiten, fondsenwerving zonder winstoogmerk en fiduciaire activiteiten, alsmede de advocatuur, mits deze activiteiten de onpartijdige uitvoering van hun ambt of de doeltreffendheid of onafhankelijkheid van de DPRC niet in de weg staan (sectie 201.7, (c), AG Regulation).

([371]) Sectie 3, (d), (iii)-(iv), EO 14086 en sectie 201.7, (d), AG Regulation.

([372]) Sectie 3, (d), (i), (D), EO 14086 en sectie 201.9, AG Regulation.

([373]) Sectie 3, (d), (iv), EO 14086 en sectie 201.7, (d), AG Regulation. Zie ook Bumap/United States, 252 U.S. 512, 515 (1920), waarin het reeds lang gehuldigde beginsel in het Amerikaanse recht wordt bevestigd dat de bevoegdheid tot ontslag voortvloeit uit de bevoegdheid tot aanstelling (waarop ook werd gewezen door het Office of Legal Counsel van het ministerie van Justitie in "The Constitutional Separation of Powers Between the President and Congress", 20 Op. O.L.C. 124, 166 (1996)).

(188) Verzoeken bij de DPRC worden beoordeeld door panels van drie rechters, waaronder een voorzittende rechter, die moeten handelen in overeenstemming met de gedragscode voor Amerikaanse rechters ([374]). Elk panel wordt bijgestaan door een bijzondere jurist (*special advocate*) ([375]), die toegang heeft tot alle informatie betreffende de zaak, met inbegrip van gerubriceerde informatie ([376]). De rol van de bijzondere jurist bestaat erin ervoor te zorgen dat de belangen van de klager worden behartigd en dat het panel van de DPRC goed wordt geïnformeerd over alle relevante juridische en feitelijke kwesties ([377]). Om zijn standpunt ten aanzien van een door een persoon bij de DPRC ingediend verzoek om toetsing nader toe te lichten, kan de bijzondere jurist informatie inwinnen bij de klager door middel van schriftelijke vragen ([378]).

(189) De DPRC toetst de vaststellingen van de CLPO van het ODNI (zowel of een schending van het toepasselijke Amerikaanse recht heeft plaatsgevonden als wat betreft de passende corrigerende maatregelen) ten minste op basis van het verslag van het onderzoek van de CLPO van het ODNI, alsook op basis van informatie en opmerkingen van de klager, de bijzondere jurist of een inlichtingendienst ([379]). Een DPRC-panel heeft toegang tot alle informatie die nodig is om een toetsing uit te voeren, die het kan verkrijgen via de CLPO van het ODNI (het panel kan de CLPO bijvoorbeeld verzoeken zijn dossier aan te vullen met aanvullende informatie of feitelijke bevindingen indien dat nodig is om de toetsing uit te voeren) ([380]).

(190) De DPRC kan aan het eind van zijn onderzoek 1) besluiten dat er geen aanwijzingen zijn dat er met betrekking tot de persoonsgegevens van de klager SIGINT-activiteiten hebben plaatsgevonden, 2) besluiten dat de vaststellingen van de CLPO van het ODNI juridisch correct waren en gestaafd werden door materieel bewijsmateriaal, of 3) indien de DPRC het niet eens is met de vaststellingen van de CLPO van het ODNI (of er een schending van de toepasselijke Amerikaanse wetgeving heeft plaatsgevonden of de passende corrigerende maatregelen), zijn eigen vaststellingen doen ([381]).

([374]) Sectie 3, (d), (i), (B), EO 14086 en sectie 201.7, (a)-(c), AG Regulation. Het Office of Privacy and Civil Liberties van het ministerie van Justitie (OPCL), dat verantwoordelijk is voor de administratieve ondersteuning van de DPRC en de bijzondere juristen (zie sectie 201.5, AG Regulation), selecteert bij toerbeurt een driekoppig panel, waarbij ervoor wordt gezorgd dat elk panel ten minste één rechter bevat met eerdere justitiële ervaring (indien geen van de rechters in het panel dergelijke ervaring heeft, is de voorzittende rechter de rechter die het eerst door het OPCL is geselecteerd).

([375]) Sectie 201.4, AG Regulation. Ten minste twee bijzondere juristen worden door de minister van Justitie, in overleg met de minister van Handel, de Director of National intelligence en de PCLOB, benoemd voor een termijn van twee jaar die kan worden verlengd. De bijzondere juristen moeten passende ervaring hebben op het gebied van privacywetgeving en wetgeving inzake de nationale veiligheid, ervaren advocaten zijn, actief lid zijn van de balie en een vergunning hebben voor de advocatuur. Bovendien mogen zij op het tijdstip van hun eerste benoeming de voorafgaande twee jaar geen werknemer van de uitvoerende macht zijn geweest. Voor elke beoordeling van een verzoek selecteert de voorzittende rechter een bijzondere jurist om het panel bij te staan, zie sectie 201.8, (a), AG Regulation.

([376]) Sectie 201.8, (c) en sectie 201.11, AG Regulation.

([377]) Sectie 3, (d), (i), (C), EO 14086 en sectie 201.8, (e), AG Regulation. De bijzondere jurist treedt niet op als vertegenwoordiger van of heeft geen advocaat-cliëntverhouding met de klager.

([378]) Zie sectie 201.8, (d), (e), AG Regulation. Dergelijke vragen worden eerst door het OPCL, in overleg met het betrokken onderdeel van de inlichtingendiensten, bestudeerd om gerubriceerde of geprivilegieerde of beschermde informatie te identificeren en uit te sluiten, alvorens ze aan de klager wordt toegezonden. Aanvullende informatie die de bijzondere jurist in antwoord op dergelijke vragen ontvangt, wordt opgenomen in de stukken van de bijzondere jurist die aan de DPRC worden gericht.

([379]) Sectie 3, (d), (i), (D), EO 14086.

([380]) Sectie 3, (d), (iii), EO 14086 en sectie 201.9, (b), AG Regulation.

([381]) Sectie 3, (d), (i), (E), EO 14086 en sectie 201.9, (c)-(e), AG Regulation. Volgens de definitie van "passende corrigerende maatregelen" in sectie 4, (a), EO 14086 moet de DPRC rekening houden met de wijze waarop een schending zoals de vastgestelde schending gewoonlijk is behandeld wanneer de DPRC beslist over een corrigerende maatregel om een schending volledig te behandelen, d.w.z. de DPRC zal, onder andere, overwegen hoe vergelijkbare nalevingskwesties in het verleden werden gecorrigeerd om ervoor te zorgen dat het rechtsmiddel doeltreffend en passend is.

(191) In alle gevallen neemt de DPRC bij meerderheid van stemmen een schriftelijk besluit. Indien de toetsing een schending van de toepasselijke regels aan het licht brengt, worden in het besluit passende corrigerende maatregelen gespecificeerd, zoals wissing van onrechtmatig verzamelde gegevens, wissing van de resultaten van onrechtmatig verrichte bevragingen, beperking van de toegang tot rechtmatig verzamelde gegevens tot naar behoren opgeleid personeel, of het terugroepen van inlichtingenrapporten die gegevens bevatten die zonder rechtmatige toestemming zijn verkregen of die onrechtmatig zijn verspreid ([382]). De beslissing van de DPRC is bindend en definitief ten aanzien van de bij hem ingediende klacht ([383]). Bovendien moet de DPRC, indien uit de toetsing een schending blijkt van een autoriteit waarop de FISC toezicht houdt, ook een gerubriceerd verslag indienen bij de adjunct-minister van Justitie voor nationale veiligheid (*Assistant Attorney General for National Security*), die op zijn beurt verplicht is de niet-naleving te melden aan de FISC, die verdere handhavingsmaatregelen kan nemen (overeenkomstig de in de overwegingen 173-174 beschreven procedure) ([384]).

(192) Elk besluit van een DPRC-panel wordt doorgegeven aan de CLPO van het ODNI ([385]). In gevallen waarin de toetsing door de DPRC op verzoek van de klager heeft plaatsgevonden, wordt de klager er via de nationale autoriteit van in kennis gesteld dat de DPRC zijn toetsing heeft afgerond en dat het onderzoek geen onder EO 14086 vallende schendingen aan het licht heeft gebracht of dat de CLPO van het ODNI een besluit heeft genomen dat passende herstelmaatregelen vereist ([386]). Het Office of Privacy and Civil Liberties van het ministerie van Justitie houdt een register bij van alle informatie die door de DPRC is onderzocht en alle besluiten die zijn genomen, dat ter beschikking wordt gesteld als niet-bindend precedent voor toekomstige DPRC-panels ([387]).

(193) Het ministerie van Handel moet ook een dossier bijhouden voor elke klager die een klacht heeft ingediend ([388]). Om de transparantie te vergroten, moet het ministerie van Handel ten minste om de vijf jaar contact opnemen met de relevante inlichtingendiensten om na te gaan of informatie met betrekking tot een toetsing door de DPRC is gederubriceerd ([389]). Indien dit het geval is, zal de betrokkene ervan in kennis worden gesteld dat dergelijke informatie beschikbaar kan zijn krachtens de toepasselijke wetgeving (d.w.z. dat hij/zij toegang kan vragen krachtens de Freedom of Information Act, zie overweging 199).

(194) Ten slotte zal de goede werking van dit verhaalmechanisme regelmatig en onafhankelijk worden geëvalueerd. Meer bepaald wordt de werking van het verhaalmechanisme overeenkomstig EO 14086 jaarlijks geëvalueerd door de PCLOB, een onafhankelijk orgaan (zie overweging 110) ([390]). Als onderdeel van deze toetsing zal de PCLOB, onder meer, beoordelen of de CLPO van het ODNI en de DPRC klachten tijdig hebben verwerkt; of zij volledige toegang hebben gekregen tot de noodzakelijke informatie; of de inhoudelijke waarborgen van EO 14086 in het toetsingsproces naar behoren in aanmerking zijn genomen; en of de inlichtingendiensten volledig hebben voldaan aan de vaststellingen van de CLPO van het ODNI en de DPRC. De PCLOB zal over het resultaat van zijn toetsing een verslag opstellen voor de president, de minister van Justitie, de Director of National Intelligence, de hoofden van de inlichtingendiensten, de CLPO van het ODNI en de inlichtingencommissies van het Congres, dat ook in een niet-gerubriceerde versie openbaar zal worden gemaakt — en dat op zijn beurt zal worden gebruikt voor de periodieke evaluatie van de werking van het huidige besluit die door de Commissie zal worden verricht. De minister van Justitie, de Director of National Intelligence, de CLPO van het ODNI en de hoofden van de inlichtingendiensten moeten alle aanbevelingen in die verslagen uitvoeren of er anderszins rekening mee houden. Bovendien zal de PCLOB jaarlijks een openbare verklaring afleggen over de vraag of het verhaalmechanisme klachten verwerkt overeenkomstig de vereisten van EO 14086.

([382]) Sectie 4, (a), EO 14086.

([383]) Sectie 3, (d), (ii), EO 14086 en sectie 201.9, (g), AG Regulation. Aangezien de beslissing van de DPRC definitief en bindend is, kan geen enkele andere uitvoerende of bestuurlijke instelling/instantie (met inbegrip van de president van de Verenigde Staten) de beslissing van de DPRC terzijde stellen. Dit werd ook bevestigd in rechtspraak van het Hooggerechtshof. met de volgende verduidelijking: de minister van Justitie heeft binnen de uitvoerende macht de unieke bevoegdheid om bindende beslissingen uit te brengen. Als de minister deze bevoegdheid aan een onafhankelijk orgaan delegeert, ontzegt hij zichzelf de mogelijkheid om de beslissing van dat orgaan op eender welke manier op te leggen (zie United States ex rel. Accardi/Shaughnessy, 347 U.S. 260 (1954).

([384]) Sectie 3, (d), (i), (F), EO 14086 en sectie 201.9, (i), AG Regulation.

([385]) Sectie 201.9, (h), AG Regulation.

([386]) Sectie 3, (d), (i), (H), EO 14086 en sectie 201.9, (h), AG Regulation. Wat de aard van de kennisgeving betreft, zie sectie 201.9, (h), (3), AG Regulation.

([387]) Sectie 201.9, (j), AG Regulation.

([388]) Sectie 3, (d), (v), (A), EO 14086.

([389]) Sectie 3, (d), (v), EO 14086.

([390]) Sectie 3, (e), EO 14086. Zie ook https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic Data Privacy Framework EO press release (FINAL).pdf

(195) Naast het bij EO 14086 ingestelde specifieke verhaalmechanisme zijn er voor alle natuurlijke personen (ongeacht hun nationaliteit of woonplaats) ook beroepsmogelijkheden voor gewone Amerikaanse rechtbanken ([391]).

(196) In het bijzonder bieden FISA en een verwante wet natuurlijke personen de mogelijkheid om langs civielrechtelijke weg een geldelijke schadevergoeding van de Verenigde Staten vorderen wanneer hen betreffende informatie onrechtmatig en opzettelijk is gebruikt of bekendgemaakt ([392]); voor de rechter een geldelijke schadevergoeding van Amerikaanse overheidsfunctionarissen in hun persoonlijke hoedanigheid te vorderen ([393]); en de wettigheid van de surveillance aan te vechten (en trachten de informatie te wissen) ingeval de Amerikaanse overheid voornemens is uit elektronische surveillance verkregen of afgeleide informatie tegen hen te gebruiken of bekend te maken in een gerechtelijke of administratieve procedure in de Verenigde Staten ([394]). Meer in het algemeen, wanneer de overheid voornemens is tijdens inlichtingenoperaties verkregen informatie te gebruiken tegen een verdachte in een strafzaak, leggen grondwettelijke en wettelijke vereisten ([395]) de verplichting op bepaalde informatie bekend te maken, zodat de verdachte de wettigheid van de verzameling en het gebruik van het bewijsmateriaal door de overheid kan aanvechten.

(197) Bovendien zijn er verschillende aanvullende mogelijkheden om gerechtelijke stappen te ondernemen tegen overheidsfunctionarissen vanwege onrechtmatige toegang van de overheid tot of gebruik door de overheid van persoonsgegevens, onder meer voor vermeende doeleinden van nationale veiligheid (te weten de Computer Fraud Abuse Act ([396]); de Electronic Communications Privacy Act ([397]); en de Right to Financial Privacy Act ([398])). Al deze rechtsvorderingen betreffen specifieke gegevens, doelen en/of soorten toegang (bv. toegang vanop afstand tot een computer via het internet) en zijn onder bepaalde voorwaarden mogelijk (bv. opzettelijke gedragingen, gedragingen buiten de officiële hoedanigheid, geleden schade).

(198) Een meer algemene verhaalmechanismemogelijkheid wordt geboden door de Administrative Procedure Act ([399]), op grond waarvan personen die onrechtmatig zijn behandeld door een overheid of die door een handeling van de overheid zijn benadeeld, zich tot het gerecht kunnen wenden ([400]). Dit omvat de mogelijkheid om van de rechterlijke instantie te vorderen dat zij vaststelt dat handelingen, vaststellingen en conclusies van de overheid willekeurig en onvoorspelbaar zijn, misbruik van discretionaire bevoegdheid inhouden of op andere wijze niet aan de wet voldoen, en dat zij die onrechtmatig en zonder gevolg verklaart ([401]). Zo oordeelde een federale *appellate court* in 2015 over een vordering uit hoofde van de APA dat de bulksgewijze verzameling van telefoniemetadata door de Amerikaanse overheid niet was toegestaan op grond van sectie 501 FISA ([402]).

([391]) De toegang tot deze beroepsmogelijkheden is afhankelijk van het aantonen van belang bij het aanhangig maken van een procedure. Deze norm, die geldt voor elke natuurlijke persoon, ongeacht diens nationaliteit, vloeit voort uit het "case or controversy"-vereiste van artikel III van de Amerikaanse grondwet. Volgens het Hooggerechtshof vereist dit dat 1) de natuurlijke persoon een "feitelijke schade" heeft geleden (d.w.z. een concrete en specifieke en actuele of dreigende schade aan een wettelijk beschermd belang), 2) er een causaal verband bestaat tussen de schade en het voor de rechter bestreden gedrag, en 3) het waarschijnlijk is, en niet speculatief, dat een gunstige beslissing van de rechter de schade zal verhelpen (zie Lujan/Defenders of Wildlife, 504 U.S. § 555 (1992)).

([392]) 18 U.S.C. § 2712.

([393]) 50 U.S.C. § 1810.

([394]) 50 U.S.C. § 1806.

([395]) Zie respectievelijk Brady/Maryland, 373 U.S. § 83 (1963) en de Jencks Act, 18 U.S.C. § 3500.

([396]) 18 U.S.C. § 1030.

([397]) 18 U.S.C. §§ 2701-2712.

([398]) 12 U.S.C. § 3417.

([399]) 5 U.S.C. § 702.

([400]) Algemeen staat alleen tegen "definitieve" handelingen van de overheid — en niet tegen "voorlopige, procedurele of tussentijdse" handelingen van de overheid — gerechtelijk verhaal open. Zie 5 U.S.C. § 704.

([401]) 5 U.S.C. § 706, (2), (A).

([402]) ACLU/Clapper, 785 F.3d 787 (2d Cir. 2015). Het in deze zaken aangevochten programma voor de bulksgewijze verzameling van telefoniegegevens werd in 2015 beëindigd door de USA Freedom Act.

(199) Naast de in de overwegingen 176 tot en met 198 genoemde verhaalmechanismemogelijkheden heeft elke natuurlijke persoon ten slotte het recht om op grond van de FOIA toegang te vragen tot bestaande documenten van federale instanties, ook wanneer deze persoonsgegevens van de natuurlijke persoon bevatten ([403]). Het verkrijgen van die toegang kan ook het instellen van procedures voor gewone rechtbanken vergemakkelijken, onder meer om het belang bij het aanhangig maken van een procedure aan te tonen. Instanties mogen informatie achterhouden die binnen bepaalde opgesomde uitzonderingen valt, waaronder toegang tot gerubriceerde informatie over de nationale veiligheid en informatie over wetshandhavingsonderzoeken ([404]), maar klagers die niet tevreden zijn met het antwoord hebben de mogelijkheid dit aan te vechten door een bestuursrechtelijke en vervolgens een rechterlijke toetsing (voor federale rechtbanken) aan te vragen ([405]).

(200) Uit het bovenstaande volgt dat wanneer Amerikaanse rechtshandhavingsinstanties en nationale veiligheidsdiensten toegang hebben tot persoonsgegevens die binnen het toepassingsgebied van dit besluit vallen, die toegang wordt geregeld door een wettelijk kader waarin de voorwaarden worden vastgesteld waaronder toegang kan plaatsvinden en wordt gewaarborgd dat de toegang en het verdere gebruik van de gegevens worden beperkt tot hetgeen noodzakelijk en evenredig is voor het nagestreefde doel inzake het openbaar belang. Deze waarborgen kunnen worden ingeroepen door natuurlijke personen die effectieve verhaalmechanismerechten genieten.

4. **CONCLUSIE**

(201) De Commissie is van mening dat de Verenigde Staten — via de door het Amerikaanse ministerie van Handel uitgevaardigde beginselen — voor persoonsgegevens die uit de Unie worden doorgegeven aan gecertificeerde organisaties in de Verenigde Staten in het kader van het EU-VS-kader voor gegevensbescherming een beschermingsniveau waarborgen dat in wezen gelijkwaardig is aan het niveau dat door Verordening (EU) 2016/679 wordt gewaarborgd.

(202) Bovendien is de Commissie van mening dat de effectieve toepassing van de beginselen wordt gewaarborgd door de transparantieverplichtingen en het beheer van het DPF door het ministerie van Handel. Bovendien maken de toezichtsmechanismen en verhaalmechanismemogelijkheden in de Amerikaanse wetgeving het over het geheel genomen mogelijk inbreuken op de gegevensbeschermingsregels op te sporen en in de praktijk te bestraffen en bieden zij de betrokkene rechtsmiddelen om toegang te krijgen tot de hem betreffende persoonsgegevens en, uiteindelijk, deze gegevens te laten rectificeren of wissen.

(203) Ten slotte is de Commissie, op basis van de beschikbare informatie over de rechtsorde van de VS, met inbegrip van de informatie in de bijlagen VI en VII, van oordeel dat elke inmenging in het algemeen belang, met name ten behoeve van de handhaving van het strafrecht en de nationale veiligheid, door overheidsinstanties van de VS in de grondrechten van de natuurlijke personen wier persoonsgegevens uit de Unie aan de Verenigde Staten worden doorgegeven op grond van het EU-VS-kader voor gegevensbescherming, beperkt zal blijven tot wat strikt noodzakelijk is om de betrokken legitieme doelstelling te bereiken, en dat er doeltreffende rechtsbescherming tegen dergelijke inmenging bestaat. In het licht van de bovenstaande bevindingen moet derhalve worden besloten dat de Verenigde Staten een passend beschermingsniveau in de zin van artikel 45 van Verordening (EU) 2016/679, uitgelegd in het licht van het Handvest van de grondrechten van de Europese Unie, waarborgen voor persoonsgegevens die vanuit de Europese Unie worden doorgegeven aan organisaties die zijn gecertificeerd op grond van het EU-VS-kader voor gegevensbescherming.

(204) Aangezien de bij EO 14086 vastgestelde beperkingen, waarborgen en het verhaalmechanisme essentiële elementen zijn van het rechtskader van de VS waarop de beoordeling van de Commissie is gebaseerd, is de vaststelling van dit besluit met name afhankelijk van de vaststelling van bijgewerkte beleidsmaatregelen en procedures ter uitvoering van EO 14086 door alle inlichtingendiensten van de VS en van de aanwijzing van de Unie als bevoegde organisatie voor de toepassing van het verhaalmechanisme, die hebben plaatsgevonden op respectievelijk 3 juli 2023 (zie overweging 126) en 30 juni 2023 (zie overweging 176).

([403]) 5 U.S.C. § 552. Soortgelijke wetten bestaan op het niveau van de staten.

([404]) Indien dit het geval is, zal de natuurlijke persoon doorgaans alleen een standaardantwoord ontvangen waarmee de dienst weigert het bestaan van gegevens te bevestigen of te ontkennen. Zie ACLU/CIA, 710 F.3d 422 (D.C. Cir. 2014). De criteria voor de rubricering en de periode waarin de rubricering van toepassing is, zijn vastgesteld in Executive Order 13526, waarin als algemene regel is gesteld dat een specifieke datum of een specifieke gebeurtenis voor derubricering moet zijn vastgesteld op grond van de periode waarin de informatie gevoelig is voor de nationale veiligheid. Vanaf die datum of op het ogenblik waarop die specifieke gebeurtenis zich voordoet, moet de informatie automatisch worden gederubriceerd (zie sectie 1.5 van EO 13526).

([405]) De rechtbank moet opnieuw beoordelen of de gegevens terecht niet zijn vrijgegeven en kan de overheid dwingen toegang tot de gegevens te verlenen (5 U.S.C § 552, (a), (4), (B)).

5. GEVOLGEN VAN DIT BESLUIT EN INGRIJPEN VAN GEGEVENSBESCHERMINGSAUTORITEITEN

(205) De lidstaten en hun organen moeten de maatregelen nemen die noodzakelijk zijn om te voldoen aan de handelingen van de instellingen van de Europese Unie, aangezien deze laatste vermoed worden rechtsgeldig te zijn en bijgevolg rechtsgevolgen in het leven roepen zolang zij niet zijn ingetrokken, nietig verklaard in een beroep tot nietigverklaring of ongeldig verklaard na een prejudiciële verwijzing of op een exceptie van onwettigheid.

(206) Daarom is een krachtens artikel 45, lid 3, van Verordening (EU) 2016/679 vastgesteld adequaatheidsbesluit van de Commissie bindend voor alle organen van de lidstaten waartoe het is gericht, met inbegrip van hun onafhankelijke toezichthoudende autoriteiten. Met name kunnen doorgiften van een verwerkingsverantwoordelijke of verwerker in de Europese Unie aan gecertificeerde organisaties in de Verenigde Staten plaatsvinden zonder dat verdere toestemming noodzakelijk is.

(207) Er zij aan herinnerd dat, overeenkomstig artikel 58, lid 5, van Verordening (EU) 2016/679 en zoals door het Hof uitgelegd in het arrest in de zaak Schrems ([406]), wanneer een nationale gegevensbeschermingsautoriteit, ook indien na ontvangst van een klacht, de verenigbaarheid van een adequaatheidsbesluit van de Commissie met de grondrechten van de persoon op privacy en gegevensbescherming in twijfel trekt, het nationale recht moet voorzien in een rechtsmiddel voor die persoon om die grieven aan een nationale rechter voor te leggen die eventueel bij prejudiciële verwijzing het Hof om beoordeling moet verzoeken ([407]).

6. TOEZICHT EN TOETSING VAN DIT BESLUIT

(208) Volgens de rechtspraak van het Hof ([408]), en zoals is erkend in artikel 45, lid 4, van Verordening (EU) 2016/679, moet de Commissie na de vaststelling van een adequaatheidsbesluit doorlopend toezicht houden op relevante ontwikkelingen in het derde land, teneinde te beoordelen of dit derde land een in wezen gelijkwaardig beschermingsniveau blijft waarborgen. Een dergelijke controle is hoe dan ook vereist wanneer de Commissie informatie ontvangt die aanleiding geeft tot gerechtvaardigde twijfel dienaangaande.

(209) Daarom moet de Commissie de situatie in de Verenigde Staten met betrekking tot het rechtskader en de feitelijke praktijk voor de verwerking van persoonsgegevens, zoals beoordeeld in dit besluit, voortdurend volgen. Om dit proces te faciliteren, moeten de Amerikaanse autoriteiten de Commissie onverwijld in kennis stellen van wezenlijke ontwikkelingen in de Amerikaanse rechtsorde die gevolgen hebben voor het rechtskader waarop dit besluit van toepassing is, alsook van ontwikkelingen in praktijken in verband met de verwerking van persoonsgegevens die in dit besluit wordt onderzocht, zowel met betrekking tot de verwerking van persoonsgegevens door gecertificeerde organisaties in de Verenigde Staten, als tot de beperkingen en waarborgen die op de toegang tot persoonsgegevens door overheidsinstanties van toepassing zijn.

(210) Teneinde de Commissie in staat te stellen haar toezichthoudende taak doeltreffend uit te voeren, moeten de lidstaten de Commissie bovendien in kennis stellen van relevante maatregelen van de nationale gegevensbeschermingsautoriteiten, met name inzake vragen of klachten van betrokkenen uit de Unie betreffende de doorgifte van persoonsgegevens vanuit de Unie aan gecertificeerde organisaties in de Verenigde Staten. Voorts moet de Commissie worden geïnformeerd over eventuele aanwijzingen dat de maatregelen van de Amerikaanse overheidsinstanties die verantwoordelijk zijn voor de preventie, het onderzoek, de opsporing of de vervolging van strafbare feiten, of voor de nationale veiligheid, met inbegrip van toezichthoudende instanties, niet het vereiste beschermingsniveau waarborgen.

([406]) Schrems, punt 65.

([407]) Schrems, punt 65: "In dat verband staat het aan de nationale wetgever om in beroepsgangen te voorzien waarmee bedoelde autoriteit de grieven die zij gegrond acht aan de nationale rechter kan voorleggen, zodat die laatste, wanneer hij de twijfel ten aanzien van de geldigheid van de beschikking van de Commissie deelt, de vraag naar de geldigheid van die beschikking prejudicieel kan verwijzen."

([408]) Schrems, punt 76.

(211) Op grond van artikel 45, lid 3, van Verordening (EU) 2016/679 ([409]) moet de Commissie na de vaststelling van dit besluit periodiek nagaan of de bevindingen betreffende de adequaatheid van het door de Verenigde Staten in het kader van het EU-VS-DPF gewaarborgde beschermingsniveau nog steeds feitelijk en juridisch gerechtvaardigd zijn. Aangezien met name EO 14086 en de AG Regulation de instelling van nieuwe mechanismen en de uitvoering van nieuwe waarborgen vereisen, moet dit besluit binnen een jaar na de inwerkingtreding ervan voor het eerst worden geëvalueerd om na te gaan of alle relevante elementen volledig zijn uitgevoerd en in de praktijk effectief functioneren. Na die eerste toetsing, en afhankelijk van het resultaat daarvan, zal de Commissie in nauw overleg met het comité dat is ingesteld bij artikel 93, lid 1, van Verordening (EU) 2016/679 en het Europees Comité voor gegevensbescherming een besluit nemen over de periodiciteit van toekomstige toetsingen ([410]).

(212) Voor de uitvoering van de toetsingen moet de Commissie bijeenkomen met het ministerie van Handel, de FTC en het ministerie van Vervoer, in voorkomend geval vergezeld van andere ministeries en instanties die betrokken zijn bij de uitvoering van het EU-VS-DPF, alsmede, voor aangelegenheden die betrekking hebben op de toegang van de overheid tot gegevens, vertegenwoordigers van het ministerie van Justitie, het ODNI (met inbegrip van de CLPO), andere onderdelen van de inlichtingendiensten, de DPRC en de bijzondere juristen (*special advocates*). Aan die bijeenkomst moet kunnen worden deelgenomen door vertegenwoordigers van de leden van het Europees Comité voor gegevensbescherming.

(213) De toetsingen moeten betrekking hebben op alle aspecten van de werking van dit besluit die verband houden met de verwerking van persoonsgegevens in de Verenigde Staten, en met name op de toepassing en uitvoering van de beginselen, met bijzondere aandacht voor de bescherming bij verdere doorgifte; relevante ontwikkelingen in de rechtspraak; de doeltreffendheid van de uitoefening van individuele rechten; het toezicht op en de handhaving van de naleving van de beginselen; alsmede de beperkingen en waarborgen met betrekking tot de toegang van de overheid, in het bijzonder de uitvoering en toepassing van de waarborgen die zijn ingevoerd bij EO 14086, ook deze die zijn ingevoerd via beleidsmaatregelen en procedures die door de inlichtingendiensten zijn ontwikkeld; de wisselwerking tussen EO 14086 en sectie 702 FISA en EO 12333; en de doeltreffendheid van de toezichtsmechanismen en de verhaalmechanismemogelijkheden (met inbegrip van de werking van het bij EO 14086 ingestelde nieuwe verhaalmechanisme). Bij dergelijke toetsingen zal er ook aandacht uitgaan naar de samenwerking tussen de gegevensbeschermingsautoriteiten en de bevoegde autoriteiten van de Verenigde Staten, met inbegrip van de ontwikkeling van richtsnoeren en andere interpretatiehulpmiddelen over de toepassing van de principes alsook andere aspecten van de werking van het kader.

(214) Op basis van de toetsing moet de Commissie een openbaar verslag opstellen dat bij het Europees Parlement en de Raad moet worden ingediend.

7. **OPSCHORTING, INTREKKING OF WIJZIGING VAN DIT BESLUIT**

(215) Wanneer uit de beschikbare informatie, met name informatie die voortvloeit uit het toezicht op dit besluit of verstrekt wordt door de autoriteiten in de Verenigde Staten of in de lidstaten, blijkt dat het beschermingsniveau voor gegevens die uit hoofde van dit besluit worden doorgegeven, wellicht niet langer passend is, moet de Commissie de bevoegde Amerikaanse autoriteiten onverwijld daarvan in kennis stellen en verzoeken dat binnen een opgegeven, redelijke termijn geschikte maatregelen worden genomen.

(216) Indien de bevoegde Amerikaanse autoriteiten die maatregelen bij het verstrijken van die opgegeven termijn niet hebben genomen of anderszins niet aannemelijk hebben kunnen maken dat dit besluit op een passend beschermingsniveau gebaseerd blijft, leidt de Commissie de in artikel 93, lid 2, van Verordening (EU) 2016/679 bedoelde procedure in teneinde dit besluit geheel of gedeeltelijk op te schorten of in te trekken.

(217) Als alternatief zal de Commissie die procedure inleiden met het oog op wijziging van dit besluit, met name door voor gegevensdoorgiften aanvullende voorwaarden te stellen of door de reikwijdte van de vaststelling van adequaatheid te beperken tot gegevensdoorgiften waarvoor een passend beschermingsniveau blijft gewaarborgd.

([409]) Artikel 45, lid 3, van Verordening (EU) 2016/679 bepaalt: "De uitvoeringshandeling voorziet in een mechanisme voor periodieke toetsing, […] waarbij alle relevante ontwikkelingen in het derde land of de internationale organisatie in aanmerking worden genomen."

([410]) Artikel 45, lid 3, van Verordening (EU) 2016/679 bepaalt dat "minstens om de vier jaar" een periodieke toetsing moet plaatsvinden. Zie ook het Europees Comité voor gegevensbescherming, Adequaatheidsreferentie, WP 254 rev. 01.

(218) De Commissie moet met name de procedure tot schorsing of intrekking in gang zetten ingeval van:

(a) aanwijzingen dat organisaties die uit hoofde van dit besluit persoonsgegevens van de Unie hebben ontvangen, de beginselen niet naleven en dat deze niet-naleving niet doeltreffend wordt aangepakt door de bevoegde toezichts- en handhavingsinstanties;

(b) aanwijzingen dat de Amerikaanse autoriteiten zich niet houden aan de toepasselijke voorwaarden en beperkingen voor de toegang van Amerikaanse overheidsinstanties ten behoeve van de rechtshandhaving en de nationale veiligheid tot persoonsgegevens die in het kader van het EU-VS-DPF worden doorgegeven; of

(c) het niet effectief behandelen van klachten van betrokkenen uit de Unie, ook niet door de CLPO van het ODNI en/of de DPRC.

(219) De Commissie moet tevens de inleiding van de procedure tot wijziging, schorsing of intrekking van dit besluit overwegen indien de bevoegde Amerikaanse autoriteiten niet de informatie of verduidelijking verstrekken die nodig is voor de beoordeling van het niveau van de bescherming van persoonsgegevens die worden doorgegeven van de Unie aan de Verenigde Staten, of van de naleving van dit besluit. In dit verband moet de Commissie rekening houden met de mate waarin relevante informatie kan worden verkregen uit andere bronnen.

(220) De Commissie zal om naar behoren gerechtvaardigde dwingende urgente redenen, bijvoorbeeld indien EO 14086 of de AG Regulation zodanig zouden worden gewijzigd dat het in dit besluit beschreven beschermingsniveau wordt ondermijnd of indien de aanwijzing door de minister van Justitie van de Unie als bevoegde organisatie voor de toepassing van het verhaalmechanisme wordt ingetrokken, gebruikmaken van de mogelijkheid om overeenkomstig de in artikel 93, lid 3, van Verordening (EU) 2016/679 bedoelde procedure onmiddellijk toepasselijke uitvoeringshandelingen tot opschorting, intrekking of wijziging van het besluit vast te stellen.

8. **SLOTOVERWEGINGEN**

(221) Het Europees Comité voor gegevensbescherming heeft zijn advies bekendgemaakt ([411]), waarmee bij het opstellen van dit besluit rekening is gehouden.

(222) Het Europees Parlement heeft een resolutie over de adequaatheid van de door het EU-VS-kader voor gegevensbescherming geboden bescherming aangenomen ([412]).

(223) De in dit besluit vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 93, lid 1, van Verordening (EU) 2016/679 ingestelde comité.

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Voor de toepassing van artikel 45 van Verordening (EU) 2016/679 waarborgen de Verenigde Staten een passend beschermingsniveau voor persoonsgegevens die vanuit de Unie worden doorgegeven aan organisaties in de Verenigde Staten die zijn opgenomen in de lijst van het kader voor gegevensbescherming (*Data Privacy Framework List*), die door het Amerikaanse ministerie van Handel (*Department of Commerce*) wordt bijgehouden en openbaar gemaakt, overeenkomstig hoofdstuk I, punt 3 van bijlage I.

Artikel 2

Wanneer de bevoegde autoriteiten in de lidstaten, om personen te beschermen in verband met de verwerking van hun persoonsgegevens, hun bevoegdheden uit hoofde van artikel 58 van Verordening (EU) 2016/679 uitoefenen met betrekking tot in artikel 1 van dit besluit bedoelde gegevensdoorgiften, stelt de betrokken lidstaat de Commissie daarvan onverwijld in kennis.

([411]) Advies 5/2023 betreffende het ontwerp van uitvoeringsbesluit van de Europese Commissie inzake het passende niveau van bescherming van persoonsgegevens krachtens het EU-VS-kader voor gegevensbescherming van 28 februari 2023.

([412]) Resolutie van het Europees Parlement van 11 mei 2023 over de gepastheid van de bescherming die wordt geboden door het kader voor gegevensbescherming EU-VS (2023/2501(RSP)).

Artikel 3

1. De Commissie houdt voortdurend toezicht op de toepassing van het rechtskader waarop dit besluit betrekking heeft, met inbegrip van de voorwaarden voor de verdere doorgifte, voor de uitoefening van individuele rechten en voor toegang van Amerikaanse overheidsinstanties tot gegevens die op basis van dit besluit worden doorgegeven, teneinde te beoordelen of de Verenigde Staten een passend beschermingsniveau als bedoeld in artikel 1 blijven waarborgen.

2. De lidstaten en de Commissie stellen elkaar in kennis van de gevallen waarin de instanties in de Verenigde Staten met de wettelijke bevoegdheid om de in bijlage I opgenomen beginselen te doen naleven, niet voorzien in doeltreffende opsporings- en toezichtsmechanismen waarmee inbreuken op de in bijlage I genoemde beginselen in de praktijk kunnen worden vastgesteld en bestraft.

3. De lidstaten en de Commissie stellen elkaar in kennis van eventuele aanwijzingen dat de ingrepen van de Amerikaanse overheidsdiensten die verantwoordelijk zijn voor de nationale veiligheid, de rechtshandhaving en andere openbare belangen, in het recht van natuurlijke personen op de bescherming van hun persoonsgegevens verder gaan dan hetgeen noodzakelijk en evenredig is, en/of dat er geen doeltreffende rechtsbescherming tegen dergelijke ingrepen is.

4. Binnen een jaar na de datum van kennisgeving van dit besluit aan de lidstaten en daarna volgens een periodiciteit waartoe zal worden besloten in nauw overleg met het comité dat is ingesteld bij artikel 93, lid 1, van Verordening (EU) 2016/679 en het Europees Comité voor gegevensbescherming, zal de Commissie de vaststelling in artikel 1, lid 1, evalueren op basis van alle beschikbare informatie, met inbegrip van de informatie die in het kader van de met de bevoegde Amerikaanse autoriteiten uitgevoerde toetsing is ontvangen.

5. Wanneer de Commissie aanwijzingen heeft dat een passend beschermingsniveau niet langer wordt gewaarborgd, stelt zij de bevoegde Amerikaanse autoriteiten daarvan in kennis. Indien noodzakelijk, zal zij, in overeenstemming met artikel 45, lid 5, van Verordening (EU) 2016/679, besluiten dit besluit te schorsen, te wijzigen of in te trekken, of de werkingssfeer ervan te beperken. De Commissie kan een dergelijk besluit ook vaststellen indien zij door het gebrek aan medewerking van de Amerikaanse regering niet kan bepalen of de Verenigde Staten een passend beschermingsniveau blijven waarborgen.

Artikel 4

Dit besluit is gericht tot de lidstaten.

Gedaan te Brussel, 10 juli 2023.

Voor de Commissie
Didier REYNDERS
Lid van de Commissie

BIJLAGE I

BEGINSELEN VAN HET EU-VS-KADER VOOR GEGEVENSBESCHERMING GEPUBLICEERD DOOR HET MINISTERIE VAN HANDEL VAN DE VERENIGDE STATEN

I. OVERZICHT

1. Hoewel de Verenigde Staten en de Europese Unie (de "EU") zich gezamenlijk inzetten voor een betere bescherming van de privacy, de rechtsstaat en een erkenning van het belang van trans-Atlantische gegevensstromen voor onze respectieve burgers, economieën en samenlevingen, hanteren de Verenigde Staten een andere benadering van gegevensbescherming dan de EU. De Verenigde Staten hebben een sectorale aanpak die is gebaseerd op een mix van wetgeving, regelgeving en zelfregulering. Het Amerikaanse ministerie van Handel ("het ministerie") vaardigt de beginselen van het EU-VS-kader voor gegevensbescherming uit, met inbegrip van de aanvullende beginselen (samen "de beginselen") en bijlage I bij de beginselen ("bijlage I"), uit hoofde van zijn wettelijke bevoegdheid om de internationale handel te bevorderen en te ontwikkelen (15 U.S.C. § 1512). De beginselen zijn ontwikkeld in overleg met de Europese Commissie ("de Commissie"), het bedrijfsleven en andere belanghebbenden om de handel tussen de Verenigde Staten en de EU te bevorderen. De beginselen, een essentieel onderdeel van het EU-VS-kader voor gegevensbescherming ("EU-VS-DPF"), bieden organisaties in de Verenigde Staten een betrouwbaar mechanisme voor de doorgifte van persoonsgegevens vanuit de EU naar de Verenigde Staten en zorgen er tegelijkertijd voor dat de betrokkenen in de EU effectieve waarborgen en bescherming blijven genieten zoals vereist door de Europese wetgeving met betrekking tot de verwerking van hun persoonsgegevens wanneer deze naar niet-EU-landen zijn doorgegeven. De beginselen zijn uitsluitend bestemd voor gebruik door in aanmerking komende organisaties in de Verenigde Staten die persoonsgegevens uit de EU ontvangen om in aanmerking te kunnen komen voor het EU-VS-DPF en aldus te profiteren van het adequaatheidsbesluit van de Commissie ([1]). De beginselen hebben geen invloed op de toepassing van Verordening (EU) 2016/679 ("de algemene verordening gegevensbescherming" of "AVG") ([2]) die van toepassing is op de verwerking van persoonsgegevens in de EU-lidstaten. Evenmin vormen de beginselen een beperking van de privacyverplichtingen die voor het overige van toepassing zijn krachtens de Amerikaanse wet.

2. Om erop te kunnen vertrouwen dat in het kader van het EU-VS-DPF de doorgifte van persoonsgegevens uit de EU wordt geëffectueerd, moet een organisatie tegenover het ministerie (of de door het ministerie aangewezen instantie) verklaren dat zij door middel van zelfcertificering de beginselen onderschrijft. Hoewel de beslissingen van organisaties om aldus deel te nemen aan het EU-VS-DPF geheel vrijwillig zijn, is de effectieve naleving ervan verplicht: organisaties die een zelfcertificeringsverklaring indienen bij het ministerie en in het openbaar verklaren de verplichting aan te gaan om zich aan de beginselen te houden, moeten de beginselen volledig in acht nemen. Teneinde deel te kunnen nemen aan het EU-VS-DPF moet een organisatie a) onderworpen zijn aan de onderzoeks- en handhavingsbevoegdheden van de Federal Trade Commission (de "FTC"), het ministerie van Vervoer van de Verenigde Staten of een andere officiële instantie die de effectieve naleving van de beginselen zal waarborgen *(andere Amerikaanse officiële organen die door de EU zijn erkend kunnen in de toekomst in bijlage worden opgenomen)*; b) in het openbaar verklaren de verplichting aan te gaan om zich aan de beginselen te houden; c) haar privacybeleid overeenkomstig deze beginselen openbaar maken; en d) dit beleid volledig uitvoeren ([3]). Wanneer een organisatie een en ander niet naleeft, kan handhavend worden opgetreden door de FTC op grond van sectie 5 van de Federal Trade Commission (FTC) Act die oneerlijke en misleidende handelingen op het gebied van of met invloed op de handel verbiedt (15 U.S.C. § 45); door het ministerie van Vervoer krachtens 49 U.S.C. § 41712, waarin het luchtvaartmaatschappijen en reisbureaus wordt verboden oneerlijke of misleidende praktijken uit te voeren bij luchtvervoer of de verkoop van luchtvervoer; of krachtens andere wetten of voorschriften die dergelijke handelingen verbieden.

([1]) Op voorwaarde dat het besluit van de Commissie inzake het passend karakter van de door het EU-VS-DPF geboden bescherming van toepassing is op IJsland, Liechtenstein en Noorwegen, zal het EU-VS-DPF op zowel de EU als deze drie landen van toepassing zijn. Bijgevolg moeten verwijzingen naar de EU en haar lidstaten ook worden gelezen als verwijzingen naar IJsland, Liechtenstein en Noorwegen.

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

([3]) De beginselen van het EU-VS-privacyschildkader zijn gewijzigd in de "beginselen van het EU-VS-kader voor gegevensbescherming". (Zie het aanvullend beginsel inzake zelfcertificering).

3. Het ministerie zal een gezaghebbende lijst bijhouden en ter beschikking van het publiek stellen, van Amerikaanse organisaties die bij het ministerie een zelfcertificeringsverklaring hebben ingediend en die hebben verklaard de beginselen te onderschrijven ("de DPF-lijst"). De voordelen van het EU-VS-DPF zijn gegarandeerd vanaf de datum dat het ministerie de organisatie op de DPF-lijst plaatst. Het ministerie zal de organisaties die zich vrijwillig terugtrekken uit het EU-VS-DPF of hun jaarlijkse hercertificering bij het ministerie niet voltooien, schrappen van de DPF-lijst; deze organisaties moeten ofwel de beginselen blijven toepassen op de persoonsgegevens die zij in het kader van het EU-VS-DPF hebben ontvangen en jaarlijks aan het ministerie bevestigen dat zij zich daartoe verbinden (d.w.z. zolang zij die informatie bewaren), ofwel de informatie op een "passende" manier beschermen op een andere toegestane wijze (bijvoorbeeld door een contract te gebruiken dat volledig voldoet aan de vereisten van de desbetreffende modelcontractbepalingen van de Commissie), of de informatie teruggeven of wissen. Het ministerie zal ook de organisaties die permanent nalaten om zich aan de beginselen te houden van de DPF-lijst verwijderen; deze organisaties moeten de persoonsgegevens die zij in het kader van het EU-VS-DPF hebben ontvangen, teruggeven of wissen. De verwijdering van een organisatie van de DPF-lijst betekent dat zij niet langer mag profiteren van het adequaatheidsbesluit van de Commissie om persoonsgegevens uit de EU te ontvangen.

4. Het ministerie zal tevens een gezaghebbende lijst bijhouden en ter beschikking van het publiek stellen van Amerikaanse organisaties die eerder wel bij het ministerie een zelfcertificering hadden ingediend, maar die van de DPF-lijst zijn verwijderd. Het ministerie zal duidelijk waarschuwen dat deze organisaties niet deelnemen aan het EU-VS-DPF; dat de verwijdering van de DPF-lijst betekent dat die organisaties niet kunnen beweren dat zij het EU-VS DPF naleven en dat zij verklaringen of misleidende praktijken moeten vermijden waaruit zou kunnen worden opgemaakt dat zij aan het EU-VS-DPF deelnemen; en dat die organisaties niet langer in aanmerking komen om te profiteren van het adequaatheidsbesluit van de Commissie om persoonsgegevens uit de EU te ontvangen. Een organisatie die blijft beweren dat zij deelneemt aan het EU-VS-DPF of een andere aan het EU-VS-DPF gerelateerde verkeerde voorstelling van zaken geeft nadat zij van de DPF-lijst is verwijderd, kan worden onderworpen aan handhavend optreden van de FTC, het ministerie van Vervoer of andere handhavingsinstanties.

5. De onderschrijving van deze beginselen kan worden beperkt: a) voor zover nodig is om te voldoen aan een rechterlijk bevel of aan eisen van openbaar belang, rechtshandhaving of nationale veiligheid, ook wanneer de wet of overheidsreglementering tegenstrijdige verplichtingen schept; b) op grond van een wet, een rechterlijk bevel of overheidsreglementering dat/die uitdrukkelijke bevoegdheden creëert, op voorwaarde dat een organisatie bij het uitoefenen van een dergelijke bevoegdheid kan aantonen dat haar niet-naleving van de beginselen niet verder gaat dan nodig is om te voldoen aan de dwingende legitieme belangen die door een dergelijke bevoegdheid worden bevorderd; of c) indien de AVG uitzonderingen of afwijkingen toestaat, onder de daarin vastgestelde voorwaarden, mits deze uitzonderingen of afwijkingen in vergelijkbare situaties worden toegepast. In dit verband omvatten de waarborgen in de Amerikaanse wetgeving ter bescherming van de privacy en de burgerlijke vrijheden de waarborgen die worden vereist door Executive Order 14086 ([4]) onder de daarin gestelde voorwaarden (met inbegrip van de eisen inzake noodzaak en evenredigheid). In overeenstemming met het doel de privacybescherming te verbeteren, moeten organisaties ernaar streven om deze beginselen volledig en op transparante wijze uit te voeren, onder meer door in hun privacybeleid te vermelden in welke gevallen uitzonderingen op de beginselen als toegestaan in punt b) van toepassing zullen zijn. Om dezelfde reden wordt, wanneer deze optie is toegestaan krachtens de beginselen en/of de Amerikaanse wet, van organisaties verwacht dat zij waar mogelijk kiezen voor de hogere mate van bescherming.

6. Organisaties zijn verplicht de beginselen toe te passen op alle persoonsgegevens die op basis van het EU-VS-DPF zijn doorgegeven nadat zij zich voor het EU-VS-DPF hebben laten registreren. Een organisatie die ervoor kiest om de voordelen van het EU-VS-DPF uit te breiden naar personeelsbeheersinformatie die vanuit de EU wordt doorgegeven voor gebruik in het kader van een arbeidsverhouding, moet dit aangeven wanneer ze een zelfcertificeringsverklaring indient bij het ministerie en moet aan de in het aanvullende beginsel inzake zelfcertificering gestelde vereisten voldoen.

([4]) Executive Order van 7 oktober 2022, "Enhancing Safeguards for United States Signals Intelligence Activities" [Executive Order tot verbetering van de waarborgen voor activiteiten van de VS op het gebied van signals intelligence (SIGINT — inlichtingen uit het berichtenverkeer)].

7. De Amerikaanse wetgeving zal van toepassing zijn op kwesties inzake de interpretatie en naleving van de beginselen en het relevante privacybeleid door de organisaties die deelnemen aan het EU-VS-DPF, behalve wanneer deze organisaties hebben toegezegd om samen te werken met de EU-gegevensbeschermingsautoriteiten. Tenzij anders aangegeven, zijn alle bepalingen van de beginselen van toepassing waar deze relevant zijn.

8. Definities:

   a. "Persoonsgegevens" en "persoonlijke informatie": de gegevens over een geïdentificeerde of identificeerbare natuurlijke persoon die binnen het toepassingsgebied van de AVG vallen en door een organisatie in de Verenigde Staten vanuit de EU worden ontvangen, en in welke vorm dan ook worden vastgelegd.

   b. "Verwerking" van persoonsgegevens: elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken of verspreiden en wissen of vernietigen.

   c. "Verwerkingsverantwoordelijke": een persoon of organisatie die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens bepaalt.

9. De datum van inwerkingtreding van de beginselen en bijlage I bij de beginselen is de datum van inwerkingtreding van het adequaatheidsbesluit van de Europese Commissie.

II. **BEGINSELEN**

1. **KENNISGEVING**

a. Een organisatie moet natuurlijke personen informeren over:

   i. haar deelname aan het EU-VS-DPF en een link verstrekken naar, of het webadres vermelden van, de DPF-lijst;

   ii. de aard van de verzamelde persoonsgegevens en, indien van toepassing, de Amerikaanse entiteiten of Amerikaanse dochterondernemingen van de organisatie die de beginselen ook onderschrijven;

   iii. haar verbintenis om de beginselen toe te passen op alle persoonsgegevens die in vertrouwen op het EU-VS-DPF vanuit de EU zijn ontvangen;

   iv. het doel waarvoor zij persoonlijke informatie over hen verzamelt en gebruikt;

   v. de wijze waarop in geval van vragen of klachten contact kan worden opgenomen met de organisatie, met inbegrip van elke relevante vestiging in de EU die kan reageren op dergelijke vragen of klachten;

   vi. het soort of de identiteit van derden aan wie zij persoonsgegevens meedeelt, en het doel waarvoor zij dat doet;

   vii. het recht van personen van toegang tot hun persoonsgegevens;

   viii. de keuzes en de middelen die de organisatie aan particulieren aanbiedt ter beperking van het gebruik en de openbaarmaking van hun persoonsgegevens;

   ix. de onafhankelijke geschillenbeslechtingsinstantie die is aangewezen om klachten te behandelen en te voorzien in passende, kosteloze verhaalsmogelijkheden voor de betrokken natuurlijke persoon, en of dat: 1) het panel is dat door gegevensbeschermingsautoriteiten is opgericht, 2) een instantie voor alternatieve geschillenbeslechting is die in de EU gevestigd is, of 3) een instantie voor alternatieve geschillenbeslechting in de Verenigde Staten is;

   x. het onderworpen zijn aan de onderzoeks-en handhavingsbevoegdheden van de FTC, het ministerie van Vervoer of een andere gemachtigde VS overheidsinstantie;

   xi. de mogelijkheid voor de natuurlijke persoon om onder bepaalde voorwaarden een beroep op bindende arbitrage te doen ([5]);

   xii. de verplichting om persoonlijke informatie bekend te maken als reactie op een gerechtvaardigd verzoek van openbare instanties, onder meer ter voldoening aan de eisen in verband met nationale veiligheid of rechtshandhaving; en

   xiii. haar aansprakelijkheid in geval van verdere doorgifte aan derde partijen.

([5]) Zie bijvoorbeeld punt c) van het beginsel inzake verhaal, handhaving en aansprakelijkheid.

b. Deze kennisgeving moet in duidelijke en ondubbelzinnige bewoordingen worden gedaan wanneer de betrokkenen voor de eerste keer wordt gevraagd de organisatie persoonlijke informatie te verstrekken of zo spoedig mogelijk daarna, maar in ieder geval voordat de organisatie dergelijke informatie gebruikt voor een ander doel dan dat waarvoor deze oorspronkelijk door de doorgevende organisatie is verzameld of verwerkt, of voordat de organisatie dergelijke informatie voor de eerste keer aan derden bekendmaakt.

2. **KEUZE**

a. Een organisatie moet natuurlijke personen de mogelijkheid geven zich ertegen te verzetten (d.w.z. opt-out) dat hun persoonlijke informatie i) aan derden bekend zal worden gemaakt of ii) zal worden gebruikt voor een doel dat wezenlijk verschilt van het (de) doel(en) waarvoor deze informatie oorspronkelijk is verzameld of waarvoor de natuurlijke persoon achteraf zijn toestemming heeft gegeven. Aan de natuurlijke persoon moeten duidelijke en opvallende, direct beschikbare mechanismen worden geboden om deze keuze te maken.

b. In afwijking van de vorige paragraaf is het niet nodig om een keuze te bieden als de informatie wordt bekendgemaakt aan een derde die optreedt als vertegenwoordiger van een organisatie om uit haar naam en in haar opdracht een of meer taken uit te voeren. Een organisatie moet echter altijd een overeenkomst met de vertegenwoordiger sluiten.

c. Voor gevoelige informatie (d.w.z. persoonlijke informatie over de gezondheid, raciale of etnische afkomst, politieke opvattingen, godsdienstige of filosofische overtuigingen, lidmaatschap van een vakbond of informatie over het seksleven van de natuurlijke persoon) moeten organisaties positieve, expliciete toestemming van de natuurlijke persoon (opt-in) krijgen, wil dergelijke informatie i) aan een derde bekend kunnen worden gemaakt of ii) kunnen worden gebruikt voor een ander doel dan waarvoor deze oorspronkelijk is verzameld of waarvoor de natuurlijke persoon achteraf zijn toestemming heeft gegeven via de uitoefening van zijn keuze voor opt-in. Bovendien moet een organisatie alle informatie die zij van een derde ontvangt en die deze derde als gevoelig aanmerkt en behandelt, als gevoelig behandelen.

3. **VERANTWOORDING VOOR DE VERDERE DOORGIFTE**

a. Wanneer een organisatie persoonlijke informatie doorgeeft aan een derde die optreedt als verwerkingsverantwoordelijke, moet zij het kennisgevingsbeginsel en het keuzebeginsel in acht nemen. Organisaties moeten ook een overeenkomst sluiten met de derde verwerkingsverantwoordelijke waarin wordt bepaald dat dergelijke gegevens uitsluitend mogen worden verwerkt voor beperkte en welomschreven doeleinden die stroken met de door de natuurlijke persoon gegeven toestemming en dat de ontvanger hetzelfde beschermingsniveau zal bieden als de beginselen en, wanneer hij vaststelt niet langer aan deze verplichting te kunnen voldoen, de organisatie daarvan in kennis stelt. In de overeenkomst wordt bepaald dat wanneer een dergelijke vaststelling plaatsvindt, de derde verwerkingsverantwoordelijke de verwerking staakt of andere redelijke en passende stappen neemt om tot een oplossing te komen.

b. In geval van doorgifte van persoonsgegevens aan een derde partij die als vertegenwoordiger handelt, mogen organisaties: i) deze gegevens uitsluitend voor beperkte en specifieke doeleinden doorgeven, en moeten zij: ii) zich ervan vergewissen dat de vertegenwoordiger verplicht is om ten minste hetzelfde niveau van privacybescherming te bieden als de beginselen voorschrijven; iii) redelijke en passende maatregelen nemen om ervoor te zorgen dat de vertegenwoordiger de doorgegeven persoonlijke informatie daadwerkelijk verwerkt op een manier die strookt met de verplichtingen van de organisatie krachtens de beginselen; iv) de vertegenwoordiger ertoe verplichten de organisatie in kennis te stellen van het feit dat hij vaststelt niet langer te kunnen voldoen aan de verplichting hetzelfde niveau van privacybescherming te bieden als de beginselen voorschrijven; v) na kennisgeving, onder meer in de zin van punt iv), redelijke en passende maatregelen nemen om de niet toegestane verwerking te stoppen en te herstellen; en vi) aan het ministerie op verzoek een samenvatting of een betrouwbare kopie overleggen van de relevante privacybepalingen van de overeenkomst met die vertegenwoordiger.

4. **VEILIGHEID**

a. Organisaties die persoonlijke informatie creëren, bewaren, gebruiken of verspreiden moeten redelijke en passende maatregelen nemen om deze te beschermen tegen verlies, misbruik en onbevoegde toegang, bekendmaking, wijziging of vernietiging, daarbij rekening houdend met de specifieke risico's in verband met de verwerking van en de aard van persoonsgegevens.

5. **INTEGRITEIT VAN GEGEVENS EN DOELBINDING**

a. Overeenkomstig de beginselen moet persoonlijke informatie worden beperkt tot de informatie die relevant is voor de doeleinden van de verwerking ([6]). Een organisatie mag geen persoonlijke informatie verwerken op een wijze die onverenigbaar is met de doeleinden waarvoor deze is verzameld of waarmee de natuurlijke persoon achteraf heeft ingestemd. Voor zover dit voor deze doeleinden noodzakelijk is, moet een organisatie redelijke stappen ondernemen om ervoor te zorgen dat de persoonsgegevens betrouwbaar zijn voor het beoogde gebruik en correct, volledig en actueel zijn. Zolang zij dergelijke informatie bewaart, moet een organisatie de beginselen in acht nemen.

b. Informatie mag worden bewaard in een vorm die de natuurlijke persoon slechts zolang identificeert of identificeerbaar ([7]) maakt als dienstig is voor het doel van verwerking in de zin van punt 5, a). Deze verplichting belet organisaties niet om persoonlijke informatie gedurende langere perioden te verwerken voor zolang en voor zover deze verwerking dienstig is ten behoeve van het archiveren in het algemeen belang, journalistiek, literatuur en kunst, wetenschappelijk of historisch onderzoek en statistische analyse. In deze gevallen zijn op deze verwerking de andere beginselen en bepalingen van het EU-VS-DPF van toepassing. Organisaties moeten redelijke en passende maatregelen nemen om aan deze bepaling te voldoen.

6. **TOEGANG**

a. Natuurlijke personen moeten toegang hebben tot de persoonlijke informatie die een organisatie over hen in bezit heeft, en moeten deze informatie, voor zover deze onjuist is of werd verwerkt in strijd met de beginselen, kunnen corrigeren, wijzigen of verwijderen, tenzij de lasten of de kosten voor het verlenen van toegang niet in verhouding staan tot het risico voor de privacy van de natuurlijke persoon, of de rechten van andere personen dan de natuurlijke persoon worden geschonden.

7. **VERHAAL, HANDHAVING EN AANSPRAKELIJKHEID**

a. Een doeltreffende privacybescherming moet ook krachtige mechanismen omvatten om de naleving van de beginselen te garanderen, alsmede verhaalsmogelijkheden voor degenen die nadeel ondervinden van de niet-naleving van de beginselen, en consequenties voor een organisatie die zich niet aan de beginselen houdt. Deze mechanismen moeten ten minste het volgende omvatten:

i. direct beschikbare, onafhankelijke en kosteloze verhaalsmechanismen voor het onderzoek en de snelle afhandeling, aan de hand van de beginselen, van klachten en geschillen van natuurlijke personen en de toekenning van schadevergoedingen wanneer het toepasselijke recht of initiatieven van de particuliere sector hierin voorzien;

ii. vervolgprocedures om na te gaan of de attesten en verklaringen van organisaties over hun privacybeleid waar zijn en of het voorgelegde beleid ter zake ook ten uitvoer is gebracht zoals is voorgesteld, met name met betrekking tot gevallen van niet-naleving; en

iii. verplichtingen om problemen op te lossen die ontstaan doordat de beginselen niet worden nageleefd door organisaties die hebben verklaard deze na te leven en consequenties voor dergelijke organisaties. De sancties moeten zwaar genoeg zijn om naleving door de organisaties te garanderen.

b. Organisaties en hun geselecteerde onafhankelijke verhaalsmechanismen moeten onmiddellijk reageren op vragen en informatieverzoeken van het ministerie in verband met het EU-VS-DPF. Alle organisaties moeten snel reageren op klachten over de naleving van de beginselen die door de autoriteiten van de EU-lidstaten via het ministerie worden ingediend. Organisaties die hebben besloten om samen te werken met de gegevensbeschermingsautoriteiten, met inbegrip van organisaties die personeelsgegevens verwerken, moeten dergelijke autoriteiten direct antwoorden wanneer het om het onderzoek en de afwikkeling van klachten gaat.

([6]) Al naargelang de omstandigheden kan het bij voorbeelden van verenigbare verwerkingsdoeleinden gaan om doeleinden die redelijkerwijze dienstig zijn voor de relatie met cliënten, overwegingen inzake naleving en juridische overwegingen, accountantscontrole, beveiliging en voorkoming van fraude, handhaving of verdediging van de wettelijke rechten van de organisatie, of andere doeleinden die, gelet op de context waarbinnen de informatie wordt verzameld, stroken met dat wat redelijkerwijs kan worden verwacht.

([7]) In dit verband is een natuurlijke persoon "identificeerbaar" wanneer, gezien de identificatiemiddelen die naar alle waarschijnlijkheid zullen worden gebruikt (onder andere gelet op de kosten van en de hoeveel tijd die nodig is voor de identificatie en de ten tijde van de verwerking beschikbare technologie) en de vorm waarin de gegevens worden bewaard, de natuurlijke persoon redelijkerwijze kan worden geïdentificeerd door de organisatie of een derde partij indien die toegang tot de gegevens zou hebben.

c. Organisaties zijn verplicht klachten aan arbitrage te onderwerpen en de voorwaarden zoals uiteengezet in bijlage I na te leven, op voorwaarde dat de natuurlijke persoon door een kennisgeving aan de betrokken organisatie en in overeenstemming met de procedures en de voorwaarden van bijlage I een beroep heeft gedaan op bindende arbitrage.

d. In het kader van een verdere doorgifte is de deelnemende organisatie verantwoordelijk voor de verwerking van de persoonlijke informatie die zij ontvangt in het kader van het EU-VS-DPF en vervolgens doorgeeft aan een derde partij die in haar naam als vertegenwoordiger optreedt. De deelnemende organisatie blijft aansprakelijk op grond van de beginselen wanneer haar vertegenwoordiger dergelijke persoonlijke informatie verwerkt op een manier die niet verenigbaar is met de beginselen, tenzij de organisatie bewijst dat zij niet verantwoordelijk is voor de gebeurtenis die de schade veroorzaakt.

e. Wanneer tegen een organisatie een rechterlijk bevel wegens niet-naleving of een bevel van een in de beginselen of in een toekomstige bijlage bij de beginselen genoemde Amerikaanse overheidsinstantie (bv. de FTC of het ministerie van Vervoer) wegens niet-naleving wordt uitgevaardigd, moet de organisatie alle relevante EU-VS-DPF-gerelateerde delen van een bij de rechter of de Amerikaanse overheidsinstantie ingediend nalevings- of beoordelingsverslag openbaar maken, voor zover dit in overeenstemming is met de vertrouwelijkheidsvereisten. Het ministerie heeft een speciaal contactpunt voor gegevensbeschermingsautoriteiten opgericht voor problemen inzake naleving door deelnemende organisaties. De FTC en het ministerie van Vervoer zullen verwijzingen inzake niet-naleving van de beginselen door het ministerie en autoriteiten van EU-lidstaten bij voorrang in overweging nemen, en tijdig informatie over de verwijzing uitwisselen met de autoriteiten van de verwijzende staat, met inachtneming van de bestaande beperkingen inzake vertrouwelijkheid.

III. AANVULLENDE BEGINSELEN

1. Gevoelige gegevens

a. Een organisatie is niet verplicht om de uitdrukkelijke bevestigende toestemming (m.a.w. een opt-in) te verkrijgen voor gevoelige gegevens, wanneer de verwerking:

i. van vitaal belang is voor de betrokkene of voor iemand anders;

ii. noodzakelijk is om rechtsvorderingen geldend te maken of om zich tegen een rechtsvordering te verweren;

iii. noodzakelijk is voor het verstrekken van medische zorg of het stellen van een diagnose;

iv. door een stichting, een vereniging of een andere instelling zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, wordt verricht in het kader van haar rechtmatige activiteiten, mits de verwerking uitsluitend betrekking heeft op de leden van die instelling of op degenen die in verband met haar doelstellingen regelmatig contact met haar onderhouden, en de gegevens niet zonder de toestemming van de betrokkenen aan derden beschikbaar worden gesteld;

v. noodzakelijk is met het oog op de uitvoering van de arbeidsrechtelijke verplichtingen van de organisatie; of

vi. betrekking heeft op gegevens waarvan duidelijk is dat ze door de natuurlijke persoon zelf openbaar zijn gemaakt.

2. Uitzonderingen voor journalistieke doeleinden

a. Gezien de in de grondwet van de Verenigde Staten neergelegde bescherming van de persvrijheid moet, wanneer de rechten van een vrije pers, die zijn opgenomen in het eerste amendement op de grondwet van de Verenigde Staten, botsen met de belangen inzake de privacybescherming, op grond van het eerste amendement ten aanzien van de activiteiten van personen of organisaties uit de Verenigde Staten een evenwicht tussen deze belangen worden gevonden.

b. Persoonlijke informatie die wordt verzameld voor publicatie, uitzending of een andere vorm van openbare communicatie van journalistiek materiaal, ook al wordt dit niet gebruikt, en informatie uit eerder gepubliceerd materiaal dat via media-archieven wordt verspreid, is niet onderworpen aan de eisen van de beginselen.

3. Secundaire aansprakelijkheid

a. Aanbieders van internetdiensten, telecommunicatiebedrijven en andere organisaties zijn niet aansprakelijk uit hoofde van de beginselen wanneer zij namens een andere organisatie informatie enkel overbrengen, routeren, schakelen of opslaan. Het EU-VS-DPF creëert geen secundaire aansprakelijkheid. Voor zover een organisatie enkel fungeert als doorgeefluik voor door derde partijen doorgegeven gegevens, zonder de doeleinden van en middelen voor de verwerking van die persoonsgegevens vast te stellen, is zij niet aansprakelijk.

4. **Uitvoeren van due diligence-onderzoek en audits**

a. De activiteiten van accountants en investeringsbankiers kunnen de verwerking van persoonsgegevens met zich brengen zonder dat de natuurlijke persoon dit weet of hiervoor toestemming heeft gegeven. Onder de hieronder beschreven omstandigheden is dit volgens de beginselen van kennisgeving, keuze en toegang toelaatbaar.

b. Naamloze en besloten vennootschappen, met inbegrip van deelnemende organisaties, worden regelmatig aan audits onderworpen. Dergelijke audits, met name die waarbij naar mogelijke onrechtmatigheden wordt gezocht, kunnen in gevaar komen als zij voortijdig bekendgemaakt worden. Zo zal ook een deelnemende organisatie die betrokken is bij een mogelijke fusie of overname een "due diligence"-onderzoek moeten uitvoeren of ondergaan. Dit zal vaak leiden tot de verzameling en verwerking van persoonsgegevens, zoals informatie over het hoger management en ander belangrijk personeel. Een te vroege bekendmaking zou de transactie kunnen belemmeren of zelfs toepasselijke effectenregelgeving kunnen schenden. Investeringsbankiers en advocaten die zich bezighouden met due diligence, of accountants die een audit uitvoeren, mogen alleen informatie verwerken zonder dat de natuurlijke persoon hiervan op de hoogte is voor zover, en gedurende de periode waarin, dit in verband met wettelijke verplichtingen of het openbaar belang noodzakelijk is, alsmede onder omstandigheden waarin de toepassing van deze beginselen de legitieme belangen van de organisatie zou schaden. Deze legitieme belangen omvatten het toezicht op de naleving door organisaties van hun wettelijke verplichtingen en wettelijk toegestane boekhoudactiviteiten, alsmede de noodzakelijke vertrouwelijkheid in verband met mogelijke overnames, fusies, joint ventures of andere soortgelijke transacties uitgevoerd door investeringsbankiers of accountants.

5. **De rol van de gegevensbeschermingsautoriteiten**

a. Organisaties zullen hun toezeggingen om met de gegevensbeschermingsautoriteiten samen te werken zoals hieronder beschreven gestand doen. In het kader van het EU-VS-DPF zijn organisaties uit de Verenigde Staten die persoonsgegevens uit de EU ontvangen, verplicht effectieve mechanismen aan te wenden om de naleving van de beginselen te waarborgen. Meer bepaald moeten de deelnemende organisaties, zoals uiteengezet in het beginsel inzake verhaal, handhaving en aansprakelijkheid voorzien in: a) i) verhaalsmogelijkheden voor degenen op wie de gegevens betrekking hebben; a) ii) vervolgprocedures om na te gaan of de attesten en verklaringen die zij over hun beleid inzake de privacybescherming hebben afgegeven, waar zijn; en a) iii) verplichtingen om problemen op te lossen die ontstaan doordat organisaties de beginselen niet naleven, en consequenties hiervan voor die organisaties. Een organisatie kan aan de punten a), i) en a), iii), van het beginsel inzake verhaal, handhaving en aansprakelijkheid voldoen, indien zij zich houdt aan de hier genoemde vereisten voor samenwerking met de gegevensbeschermingsautoriteiten.

b. Een organisatie verplicht zich ertoe met de gegevensbeschermingsautoriteiten samen te werken door in haar zelfcertificeringsverklaring inzake het EU-VS-DPF bij het ministerie te verklaren (zie het aanvullend beginsel inzake zelfcertificering) dat zij:

i. ervoor kiest aan de verplichtingen van de punten a), i) en a), iii), van het beginsel inzake verhaal, handhaving en aansprakelijkheid te voldoen door te beloven met de gegevensbeschermingsautoriteiten samen te werken;

ii. met de gegevensbeschermingsautoriteiten zal samenwerken bij het onderzoek en de oplossing van klachten die in het kader van het beginselen worden ingediend; en

iii. gevolg zal geven aan elk door de gegevensbeschermingsautoriteiten verstrekt advies als deze van oordeel zijn dat de organisatie specifieke maatregelen moet nemen om aan de beginselen te voldoen, daaronder begrepen corrigerende en compenserende maatregelen ten gunste van natuurlijke personen die schade ondervinden door niet-naleving van de beginselen, en de gegevensbeschermingsautoriteiten schriftelijk zal bevestigen dat dergelijke maatregelen zijn genomen.

c. Functioneren van panels van gegevensbeschermingsautoriteiten

i. De gegevensbeschermingsautoriteiten zullen op de volgende wijze hun medewerking verlenen in de vorm van informatie en advies:

1. het advies van de gegevensbeschermingsautoriteiten zal worden verstrekt via een informeel panel van gegevensbeschermingsautoriteiten op EU-niveau, dat onder meer zal helpen een geharmoniseerde en samenhangende aanpak te waarborgen.

2. Het panel zal aan de betrokken organisaties uit de Verenigde Staten advies uitbrengen over onopgeloste klachten van natuurlijke personen over de behandeling van persoonlijke informatie die vanuit de EU in het kader van het EU-VS-DPF is doorgegeven. Dit advies zal zo zijn opgesteld dat ervoor wordt gezorgd dat de beginselen correct worden toegepast en het zal de rechtsmiddelen voor de natuurlijke persoon/personen noemen die volgens de gegevensbeschermingsautoriteiten passend zijn.

3. Het panel zal dit advies uitbrengen naar aanleiding van verwijzingen door de betrokken organisaties en/of van rechtstreeks van natuurlijke personen ontvangen klachten tegen organisaties die zich ertoe verplicht hebben om in het kader van de doelstellingen van het EU-VS-DPF met de gegevensbeschermingsautoriteiten samen te werken. Het zal deze personen in eerste instantie aanmoedigen gebruik te maken van eventueel door de organisatie aangeboden interne regelingen voor de behandeling van klachten en hen hierbij zo nodig helpen.

4. Het panel zal pas advies uitbrengen nadat beide partijen in een geschil een redelijke kans hebben gekregen om commentaar te geven en alle gewenste bewijzen te leveren. Het zal proberen dit advies zo snel te geven als een eerlijke rechtsgang toelaat. In de regel zal het panel ernaar streven advies te verstrekken binnen 60 dagen na ontvangst van een klacht of verwijzing en zo mogelijk sneller.

5. Het panel zal de resultaten van zijn onderzoek van ingediende klachten openbaar maken als het dit gepast acht.

6. Het panel en de afzonderlijke gegevensbeschermingsautoriteiten zijn in generlei opzicht aansprakelijk voor het advies dat het panel geeft.

ii. Zoals hierboven vermeld, moeten organisaties die deze optie voor de oplossing van geschillen kiezen, zich ertoe verplichten gevolg te geven aan het advies van de gegevensbeschermingsautoriteiten. Als een organisatie niet binnen 25 dagen nadat een advies is uitgebracht, gevolg geeft aan dit advies en hiervoor geen bevredigende verklaring geeft, zal het panel kennis geven van zijn voornemen om hetzij — in gevallen van bedrog of onjuiste verklaringen — de zaak voor te leggen aan de FTC, het ministerie van Vervoer of een andere instantie van de Verenigde Staten op federaal of staatsniveau met wettelijke bevoegdheden om dwangmaatregelen te nemen, hetzij te concluderen dat de samenwerkingsovereenkomst ernstig is geschonden en bijgevolg nietig is. In het laatste geval zal het panel het ministerie hiervan op de hoogte brengen zodat de DPF-lijst dienovereenkomstig kan worden gewijzigd. Elke niet-nakoming van de verplichting om met de gegevensbeschermingsautoriteiten samen te werken, alsmede elke niet-naleving van de beginselen kan op grond van sectie 5 van de FTC Act (15 U.S.C. § 45), 49 U.S.C. § 41712, of andere soortgelijke wetten als misleidende praktijk worden vervolgd.

d. Een organisatie die wil dat haar EU-VS-DPF-bepalingen van toepassing zijn op personeelsgegevens die vanuit de EU zijn doorgegeven in het kader van een arbeidsverhouding, moet zich ertoe verplichten om met de gegevensbeschermingsautoriteiten samen te werken in verband met dergelijke gegevens (zie het aanvullend beginsel inzake personeelsgegevens).

e. Organisaties die voor deze optie kiezen, zullen een jaarlijkse bijdrage moeten betalen, die bedoeld is om de werkingskosten van het panel te dekken. Bovendien kan van hen worden verlangd dat zij de noodzakelijke vertaalkosten dragen die voortvloeien uit de behandeling door het panel van tegen hen gerichte verwijzingen of klachten. Het bedrag van de vergoeding wordt door het ministerie vastgesteld na overleg met de Commissie. De inning van de vergoeding kan worden verricht door een door het ministerie geselecteerde derde partij die als bewaarder van de voor dit doel geïnde gelden optreedt. Het ministerie zal nauw met de Commissie en de gegevensbeschermingsautoriteiten samenwerken bij de vaststelling van passende procedures voor de verdeling van de via de vergoeding geïnde middelen, alsook bij andere procedurele en administratieve aspecten van het panel. Het ministerie en de Commissie kunnen overeenkomen de frequentie van de inning van de vergoeding te wijzigen.

6. **Zelfcertificering**

a. De voordelen van het EU-VS-DPF zijn gegarandeerd vanaf de datum dat het ministerie de organisatie op de DPF-lijst plaatst. Het ministerie zal een organisatie pas op de DPF-lijst plaatsen nadat het heeft vastgesteld dat de organisatie haar eerste zelfcertificering volledig heeft ingediend, en zal de organisatie van die lijst schrappen als zij zich vrijwillig terugtrekt, haar jaarlijkse hercertificering niet voltooit of de beginselen permanent niet naleeft (zie aanvullend beginsel inzake geschillenbeslechting en handhaving).

b. Om een eerste zelfcertificering of vervolgens een hercertificering voor het EU-VS-DPF te verkrijgen, moet een organisatie het ministerie telkens een verklaring voorleggen van een directielid namens de organisatie die een zelfcertificering of hercertificering (naargelang van het geval) van haar naleving van de beginselen ([8]) uitvoert, die ten minste de volgende informatie bevat:

([8]) De aanvraag moet via de DPF-website van het ministerie worden ingediend door een natuurlijke persoon binnen de organisatie die gemachtigd is om namens de organisatie en haar betrokken entiteiten verklaringen af te leggen over de naleving van de beginselen.

i. de naam van de Amerikaanse zelfcertificerende of hercertificerende organisatie, alsmede de naam/namen van haar entiteiten in de VS of haar dochterondernemingen in de VS die eveneens de beginselen onderschrijven die de organisatie wil onderschrijven;

ii. een beschrijving van de activiteiten van de organisatie met betrekking tot de persoonsgegevens die zij uit de EU uit hoofde van het EU-VS-DPF ontvangt;

iii. een beschrijving van het relevante privacybeleid van de organisatie ten aanzien van dergelijke persoonlijke informatie, waaronder:

1. indien de organisatie een publiek toegankelijke website heeft, het desbetreffende internetadres waar het privacybeleid beschikbaar is, of indien de organisatie geen publiek toegankelijke website heeft, de mededeling waar het publiek het privacybeleid kan inzien; en

2. de datum van inwerkingtreding;

iv. een instantie binnen de organisatie waartoe men zich kan wenden voor de behandeling van klachten, verzoeken om toegang en alle andere kwesties die zich voordoen in het kader van de beginselen ([9]), waaronder:

1. de naam (namen), functie(s) (indien van toepassing), e-mailadres(sen) en telefoonnummer(s) van de natuurlijke persoon (personen) of het (de) relevante instantie(s) binnen de organisatie; en

2. het relevante Amerikaanse postadres van de organisatie;

v. de officiële instantie die bevoegd is om tegen de organisatie ingediende claims in verband met eventuele oneerlijke of misleidende praktijken en schendingen van wetten of regelingen betreffende de privacybescherming te behandelen (en die wordt vermeld in de bijlage bij de beginselen of een toekomstige bijlage bij de beginselen);

vi. de naam van privacyprogramma's waaraan de organisatie deelneemt;

vii. de verificatiemethode (d.w.z. zelfbeoordeling; of externe nalevingscontroles, met inbegrip van de derde die dergelijke controles uitvoert) ([10]); en

viii. de relevante onafhankelijke verhaalsmechanismen die beschikbaar zijn voor het onderzoeken van onopgeloste klachten in verband met de beginselen ([11]).

c. Als een organisatie wil dat personeelsgegevens die vanuit de EU in het kader van een arbeidsverhouding zijn doorgegeven, eveneens onder de voordelen van het EU-VS-DPF vallen, kan zij dit bewerkstelligen indien een in de bijlage of toekomstige bijlage bij de beginselen vermelde officiële instantie bevoegd is om tegen de organisatie ingebrachte klachten in verband met de verwerking van personeelsgegevens te behandelen. Bovendien moet de organisatie dit bij de indiening van haar eerste zelfcertificering, alsook bij de indiening van hercertificeringen, aangeven en verklaren zich ertoe te verplichten samen te werken met de EU-autoriteiten of de betrokken autoriteiten in overeenstemming met de aanvullende beginselen inzake personeelsgegevens en de rol van de gegevensbeschermingsautoriteiten, waar van toepassing, en dat zij de adviezen van deze autoriteiten zal naleven. De organisatie moet het ministerie ook een kopie verstrekken van haar privacybeleid inzake personeelsbeheer en meedelen waar het privacybeleid door de betrokken werknemers kan worden ingezien.

([9]) De primaire "contactpersoon van de organisatie" of het "directielid van de organisatie" mag niet van buiten de organisatie afkomstig zijn (bv. een externe raadsman of een externe consultant).

([10]) Zie het aanvullend beginsel inzake verificatie.

([11]) Zie het aanvullend beginsel inzake geschillenbeslechting en handhaving.

d. Het ministerie zal de DPF-lijst bijhouden en openbaar maken van organisaties die een volledige, eerste zelfcertificering hebben ingediend, en zal die lijst bijwerken op basis van volledige, jaarlijkse hercertificeringsaanvragen, alsook van kennisgevingen die worden ontvangen overeenkomstig het aanvullend beginsel inzake geschillenbeslechting en handhaving. Dergelijke hercertificeringen moeten minstens een keer per jaar worden ingediend; zo niet dan wordt de organisatie van de DPF-lijst verwijderd en zijn de voordelen van het EU-VS-DPF niet langer gegarandeerd. Alle organisaties die door het ministerie op de DPF-lijst worden geplaatst, moeten een relevant privacybeleid hebben dat voldoet aan het kennisgevingsbeginsel en in dat privacybeleid verklaren dat zij de beginselen naleven ([12]). In het privacybeleid van een organisatie moet, indien dat online beschikbaar is, een link staan naar de DPF-website van het ministerie en een link naar de website of het klachtenformulier van het onafhankelijke verhaalsmechanisme dat beschikbaar is voor het onderzoeken van onopgeloste klachten in verband met de beginselen, zonder kosten voor de natuurlijke persoon.

e. De beginselen zijn van toepassing onmiddellijk na de zelfcertificering. Deelnemende organisaties die zich voorheen zelf hebben gecertificeerd voor de beginselen van het EU-VS-privacyschildkader, moeten hun privacybeleid aanpassen en in plaats daarvan verwijzen naar de beginselen van het EU-VS-kader voor gegevensbescherming. Deze organisaties nemen deze verwijzing zo spoedig mogelijk op, en in ieder geval uiterlijk drie maanden na de datum van inwerkingtreding van de beginselen van het EU-VS-kader voor gegevensbescherming.

f. Een organisatie moet de beginselen toepassen op alle vanuit de EU op basis van het EU-VS-DPF ontvangen persoonsgegevens. Voor persoonsgegevens die worden ontvangen tijdens de periode waarin de organisatie de voordelen van het EU-VS-DPF geniet, is de verplichting de beginselen na te leven niet in de tijd beperkt; deze beginselen blijven op die gegevens van toepassing zolang de organisatie ze opslaat, gebruikt of openbaar maakt, zelfs indien de organisatie nadien om enigerlei reden niet langer aan het EU-VS-DPF deelneemt. Een organisatie die zich uit het EU-VS-DPF wenst terug te trekken, moet het ministerie daarvan vooraf in kennis stellen. Deze kennisgeving moet ook aangeven wat de organisatie zal doen met de persoonsgegevens die zij op grond van het EU-VS-DPF heeft ontvangen (d.w.z. de gegevens bewaren, terugzenden of wissen, en indien zij de gegevens bewaart, de toegestane middelen waarmee zij de gegevens zal beschermen). Een organisatie die niet langer deelneemt aan het EU-VS-DPF, maar dergelijke gegevens wenst te behouden, moet ofwel jaarlijks aan het ministerie bevestigen dat zij zich ertoe verbindt de beginselen te zullen blijven toepassen op de gegevens ofwel op een andere geautoriseerde wijze "passende" bescherming voor de gegevens bieden (bijvoorbeeld met behulp van een overeenkomst die de voorschriften van de door de Commissie vastgestelde relevante modelcontractbepalingen volledig weergeeft); anders moet de organisatie de informatie terugsturen of wissen ([13]). Een organisatie die niet langer deelneemt aan het EU-VS-DPF moet, waar relevant, in haar privacybeleid alle verwijzingen naar het EU-VS-DPF verwijderen die de indruk wekken dat ze nog steeds actief deelneemt aan EU-VS-DPF en recht heeft op de voordelen ervan.

([12]) Een organisatie die voor het eerst een zelfcertificering indient, mag in haar definitieve privacybeleid geen aanspraak maken op deelname aan het EU-VS-DPF totdat het ministerie de organisatie meedeelt dat zij dit mag doen. De organisatie moet het ministerie bij de indiening van haar eerste zelfcertificering een ontwerp-privacybeleid voorleggen dat in overeenstemming is met de beginselen. Zodra het ministerie heeft vastgesteld dat de eerste zelfcertificering van de organisatie voor het overige volledig is, zal het de organisatie meedelen dat zij haar EU-VS-DPF-conforme privacybeleid moet afronden (bv. publiceren indien van toepassing). De organisatie moet het ministerie onmiddellijk op de hoogte brengen zodra het desbetreffende privacybeleid is afgerond, waarna het ministerie de organisatie op de DPF-lijst zal plaatsen.

([13]) Indien een organisatie er bij de terugtrekking voor kiest de persoonsgegevens die zij op grond van het EU-VS-DPF heeft ontvangen, te bewaren en jaarlijks aan het ministerie bevestigt dat zij de beginselen op die gegevens blijft toepassen, moet de organisatie het ministerie eenmaal per jaar na de terugtrekking (d.w.z. tenzij en totdat de organisatie op een andere toegestane wijze een "passende" bescherming voor die gegevens biedt, of al die gegevens teruggeeft of wist en het ministerie daarvan in kennis stelt) aantonen wat zij met die persoonsgegevens heeft gedaan, wat zij zal doen met de persoonsgegevens die zij blijft bewaren, en wie als permanent contactpunt zal fungeren voor vragen in verband met de beginselen.

g. Een organisatie die haar rechtspersoonlijkheid als zelfstandige onderneming zal verliezen door een verandering in de bedrijfsstatus, bijvoorbeeld als gevolg van een fusie, overname, faillissement of ontbinding, moet het ministerie hiervan vooraf in kennis stellen. In de kennisgeving moet ook worden aangegeven of de uit de wijziging van de bedrijfsstatus voortvloeiende entiteit i) via een bestaande zelfcertificering zal blijven deelnemen aan het EU-VS-DPF; ii) zichzelf zal certificeren als nieuwe deelnemer aan het EU-VS-DPF (bv. wanneer de nieuwe entiteit of de overlevende entiteit niet reeds over een bestaande zelfcertificering beschikt waarmee zij aan het EU-VS-DPF zou kunnen deelnemen); of iii) andere waarborgen zal invoeren, zoals een schriftelijke overeenkomst die garandeert dat de beginselen blijvend worden toegepast op alle persoonsgegevens die de organisatie in het kader van het EU-VS-DPF heeft ontvangen en die zullen worden bewaard. Als noch i), noch ii), noch iii) van toepassing is, moeten alle persoonsgegevens die in het kader van het EU-VS-DPF zijn verkregen, onmiddellijk worden teruggegeven of gewist.

h. Wanneer een organisatie om welke reden dan ook niet langer aan het EU-VS-DPF deelneemt, moet zij alle verklaringen verwijderen waaruit zou kunnen worden opgemaakt dat zij aan het EU-VS-DPF blijft deelnemen of recht heeft op de voordelen van het EU-VS-DPF. Het EU-VS-DPF-keurmerk, indien gebruikt, moeten eveneens worden geschrapt. De FTC, het ministerie van Vervoer of een andere bevoegde overheidsinstantie kan actie ondernemen tegen iedere onjuiste verklaring aan het grote publiek met betrekking tot de naleving van de beginselen door een organisatie. In geval van onjuiste verklaringen tegenover het ministerie kan vervolging worden ingesteld op grond van de False Statements Act (18 U.S.C. § 1001).

7. **Verificatie**

a. Organisaties moeten in vervolgprocedures voorzien om na te gaan of de attesten en verklaringen die zij over hun beleid inzake privacybescherming in het kader van het EU-VS-DPF afleggen, waar zijn en of dit beleid is uitgevoerd zoals het is voorgesteld en of het beantwoordt aan de beginselen.

b. Teneinde aan de controle-eisen van het beginsel inzake verhaal, handhaving en aansprakelijkheid te voldoen, moet een organisatie de naleving van dergelijke attesten en verklaringen door middel van zelfbeoordeling of door externe nalevingscontroles nagaan.

c. Wanneer de organisatie voor zelfbeoordeling heeft gekozen, moet deze verificatie aantonen dat haar privacybeleid met betrekking tot uit de EU ontvangen persoonsgegevens nauwkeurig, volledig en direct beschikbaar is, voldoet aan de beginselen en volledig wordt uitgevoerd (d.w.z. dat het wordt nageleefd). Voorts moet blijken dat natuurlijke personen in kennis worden gesteld van interne regelingen voor de behandeling van klachten en van de onafhankelijke verhaalsmechanismen om klachten in te dienen; dat de organisatie haar werknemers opleidt op het gebied van de uitvoering van het beleid en dat er tuchtmaatregelen tegen hen worden genomen indien zij dit beleid niet volgen; en dat er voorts interne procedures zijn om periodiek objectief na te gaan of het bovenstaande ook wordt nageleefd. Een verklaring ter bevestiging dat de zelfbeoordeling is voltooid, moet minstens eens per jaar door een directielid of een andere daartoe bevoegde vertegenwoordiger van de organisatie worden ondertekend en op verzoek aan natuurlijke personen of in het kader van een onderzoek of een klacht wegens niet-naleving ter beschikking worden gesteld.

d. Wanneer de organisatie voor externe beoordeling van de naleving heeft gekozen, moet deze verificatie aantonen dat haar privacybeleid met betrekking tot uit de EU ontvangen persoonsgegevens nauwkeurig, volledig en direct beschikbaar is, voldoet aan de beginselen en volledig wordt uitgevoerd (d.w.z. dat het wordt nageleefd). Er moet ook worden aangegeven dat natuurlijke personen worden geïnformeerd over de mechanismen via welke zij klachten kunnen indienen. De controlemethoden mogen zonder beperking audits, steekproeven, het gebruik van "valstrikken" of het gebruik van technologische middelen omvatten. Een verklaring omtrent de uitvoering van de externe controle moet eens per jaar door de controleur of een directielid of een andere daartoe bevoegde vertegenwoordiger van de organisatie worden ondertekend en op verzoek aan natuurlijke personen of in het kader van een onderzoek of een klacht wegens niet-naleving ter beschikking worden gesteld.

e. Organisaties moeten hun informatiebestanden over de uitvoering van hun beleid inzake de bescherming van de privacy in het kader van het EU-VS-DPF bewaren en deze bij een onderzoek of een klacht wegens niet-naleving op verzoek ter beschikking stellen aan de onafhankelijke geschillenbeslechtingsinstantie die met het onderzoek van klachten belast is of aan de instantie die oneerlijke en misleidende praktijken moet onderzoeken. Ook moeten organisaties onmiddellijk reageren op vragen en andere informatieverzoeken van het ministerie in verband met de onderschrijving door de organisatie van de beginselen.

8. **Toegang**

a. Het beginsel van toegang in de praktijk

i. Volgens de beginselen is het recht van toegang fundamenteel voor de privacybescherming. Met name geeft dit recht de betrokkene de mogelijkheid om de juistheid van de informatie die over hem wordt bijgehouden, na te gaan. Het beginsel van toegang houdt in dat natuurlijke personen het recht hebben om:

1. van een organisatie een bevestiging te ontvangen of de organisatie al dan niet persoonsgegevens verwerkt die op hen betrekking hebben ([14]);

2. dergelijke gegevens aan hen te doen meedelen opdat zij kunnen controleren of zij nauwkeurig zijn en de verwerking ervan rechtmatig is; en

3. de gegevens te laten corrigeren, wijzigen of schrappen wanneer ze niet nauwkeurig zijn of werden verwerkt in strijd met de beginselen.

ii. Natuurlijke personen behoeven een verzoek om toegang tot hun eigen gegevens niet te motiveren. Organisaties moeten zich bij hun reactie op een verzoek van een natuurlijke persoon om toegang om te beginnen afvragen waarom de betrokkene zijn verzoek heeft ingediend. Indien een verzoek bijvoorbeeld in vage of algemene bewoordingen is gesteld, kan de organisatie beter een dialoog met de natuurlijke persoon aangaan om de achterliggende reden voor het verzoek beter te begrijpen, om aldus vast te stellen welke informatie relevant is. De organisatie kan bijvoorbeeld nagaan met welke afdeling(en) van de organisatie de natuurlijke persoon contact heeft gehad of voor welk soort informatie of gebruik daarvan toegang wordt gevraagd.

iii. Gezien het fundamentele karakter van toegang, mogen organisaties de toegang nooit zonder meer beperken. Als bijvoorbeeld bepaalde informatie moet worden beschermd, maar probleemloos kan worden gescheiden van andere persoonlijke informatie waarvoor toegang is gevraagd, moet de organisatie de beschermde informatie bewerken en de andere informatie beschikbaar stellen. Indien een organisatie besluit dat de toegang in een bepaald geval moet worden beperkt, moet zij de betrokkene die om toegang verzoekt, uitleggen waarom zij tot dit besluit is gekomen en een contactadres opgeven waar de natuurlijke persoon met vragen terechtkan.

b. Lasten of kosten inzake het verschaffen van toegang

i. Het recht op toegang tot persoonsgegevens kan in uitzonderlijke omstandigheden worden beperkt en wel indien de wettelijke rechten van andere personen dan de natuurlijke persoon zouden worden geschonden of wanneer de aan het verschaffen van toegang verbonden lasten en kosten onevenredig zouden zijn gelet op de risico's in de zaak in kwestie voor de privacy van de natuurlijke persoon. Kosten en lasten zijn belangrijke factoren die in overweging moeten worden genomen, maar zij zijn geen doorslaggevende factoren bij een beslissing over de redelijkheid van toegang.

ii. Indien de persoonlijke informatie bijvoorbeeld gebruikt wordt voor beslissingen die voor de natuurlijke persoon van groot belang zijn (zoals het weigeren of toekennen van belangrijke voordelen, zoals een verzekering, een hypotheek of een baan), dan moet de organisatie, in overeenstemming met de andere bepalingen van deze aanvullende beginselen, deze informatie ter beschikking stellen, ook al is dit vrij moeilijk of duur. Indien de gevraagde persoonlijke informatie niet gevoelig is of niet wordt gebruikt voor beslissingen die voor de natuurlijke persoon van groot belang zijn, maar meteen beschikbaar is en zonder noemenswaardige kosten kan worden gegeven, dan moet de organisatie toegang tot dergelijke informatie verlenen.

c. Vertrouwelijke commerciële informatie

i. Vertrouwelijke commerciële informatie is informatie die door een organisatie tegen openbaarmaking wordt beschermd en waarvan de openbaarmaking concurrenten op de markt zou helpen. Organisaties kunnen de toegang tot informatie ontzeggen of beperken voor zover het verlenen van volledige toegang zou leiden tot onthulling van hun eigen vertrouwelijke commerciële informatie, zoals door de organisatie opgestelde marketingconclusies of classificaties, of van de vertrouwelijke commerciële informatie van een andere organisatie waarop een contractuele geheimhoudingsplicht van toepassing is.

([14]) De organisatie moet antwoorden op vragen van natuurlijke personen over de doeleinden van de verwerking, de categorieën persoonsgegevens waarop de verwerking betrekking heeft en de ontvangers of categorieën ontvangers aan wie de gegevens worden verstrekt.

ii. Wanneer het mogelijk is vertrouwelijke commerciële informatie probleemloos te scheiden van andere persoonlijke informatie waarvoor toegang is gevraagd, moet de organisatie de vertrouwelijke commerciële informatie bewerken en de niet-vertrouwelijke informatie beschikbaar stellen.

d. Organisatie van databanken

i. Toegang kan worden verleend doordat een organisatie de natuurlijke persoon de betreffende persoonlijke informatie ter beschikking stelt en vereist niet dat de natuurlijke persoon toegang krijgt tot de databank van een organisatie.

ii. Een organisatie behoeft alleen toegang tot door haar opgeslagen persoonlijke informatie te verlenen. Het toegangsbeginsel houdt geen verplichting in om bestanden met persoonlijke informatie te bewaren, te onderhouden, te reorganiseren of te herstructureren.

e. Wanneer kan de toegang worden beperkt

i. Aangezien organisaties zich altijd te goeder trouw moeten inspannen om natuurlijke personen toegang tot hun persoonsgegevens te geven, is er maar een bepaald aantal situaties waarin zij een dergelijke toegang mogen beperken en moeten er concrete redenen voor een dergelijke beperking zijn. Net zoals in het kader van de AVG kan een organisatie toegang tot informatie beperken, wanneer belangrijke openbare belangen, zoals de nationale of openbare veiligheid, of de defensie hiermee in strijd zijn. Indien persoonlijke informatie uitsluitend wordt verwerkt voor statistische of onderzoeksdoeleinden kan de toegang eveneens worden geweigerd. Andere redenen om de toegang te weigeren of te beperken zijn:

1. de openbaarmaking belemmert de uitvoering of de handhaving van de wet of van civielrechtelijke procedures, inclusief het voorkomen, onderzoeken of opsporen van misdrijven, of van het recht op een eerlijk proces;

2. de openbaarmaking schendt de legitieme rechten of gewichtige belangen van anderen;

3. de openbaarmaking schendt beroepsrechten of -plichten die al dan niet voortvloeien uit de wet;

4. de openbaarmaking conflicteert met veiligheidsonderzoeken of klachtenprocedures waarbij werknemers zijn betrokken of in verband met personeelsbeleid en bedrijfsherstructureringen; of

5. aantasting van de geheimhouding die noodzakelijk is voor toezichthoudende of regulerende taken in verband met een gezond beheer of bij toekomstige of lopende onderhandelingen met betrekking tot de organisatie.

ii. Een organisatie die zich op een uitzondering beroept, moet aantonen dat die uitzondering noodzakelijk is en aan natuurlijke personen de redenen voor het beperken van de toegang meedelen alsook een contactadres opgeven waar zij met verdere vragen terechtkunnen.

f. Het recht om een bevestiging te krijgen en de kosten voor het verlenen van toegang in rekening te brengen

i. Een natuurlijk persoon heeft het recht om een bevestiging te verkrijgen of een organisatie al of niet persoonsgegevens over hem of haar heeft. Een natuurlijk persoon heeft er eveneens recht op dat haar of hem de haar of hem betreffende persoonsgegevens worden meegedeeld. Een organisatie mag alleen een vergoeding vragen die niet buitensporig is.

ii. Het vragen van een vergoeding kan bijvoorbeeld gerechtvaardigd zijn wanneer verzoeken om toegang kennelijk buitensporig zijn, met name vanwege hun repetitief karakter.

iii. De toegang kan niet op grond van de kosten worden geweigerd als de natuurlijke persoon aanbiedt deze kosten te betalen.

g. Repetitieve of vexatoire verzoeken om toegang

i. Een organisatie kan redelijke grenzen stellen aan het aantal keren dat binnen een bepaalde periode aan verzoeken om toegang van een bepaalde persoon zal worden voldaan. Bij het vaststellen van dergelijke beperkingen moet een organisatie rekening houden met factoren als de frequentie waarmee informatie wordt bijgewerkt, het doel waarvoor de gegevens worden gebruikt en de aard van de informatie.

h. Frauduleuze verzoeken om toegang

i. Een organisatie behoeft alleen toegang te verlenen wanneer het verzoek gepaard gaat met voldoende informatie om haar in staat te stellen de identiteit van de verzoeker vast te stellen.

i. Tijdschema voor reacties

i. Op verzoeken om toegang moeten organisaties reageren binnen een redelijke termijn, op een redelijke wijze en in een vorm die voor de natuurlijke persoon eenvoudig te begrijpen is. Een organisatie die met regelmaat informatie aan de betrokkenen verstrekt, kan aan een individueel verzoek om toegang voldoen via deze regelmatige openbaarmaking mits dat geen buitensporige vertraging met zich brengt.

9. **Personeelsgegevens**

a. Dekking door het EU-VS-DPF

i. Wanneer een organisatie in de EU persoonlijke informatie over haar (voormalige of huidige) werknemers, die zij in het kader van een arbeidsverhouding heeft verzameld, doorgeeft aan een moederorganisatie, dochterorganisatie of een niet-geaffilieerde dienstverlener in de Verenigde Staten die aan het EU-VS-DPF deelneemt, zijn de beginselen van het EU-VS-DPF op deze doorgifte van toepassing. In deze gevallen was de nationale wetgeving van de EU-lidstaat waar de informatie werd verzameld, van toepassing op het verzamelen en verwerken van de informatie voordat deze werd doorgegeven, en moeten alle voorwaarden voor of restricties op de doorgifte die deze wetgeving stelt, in acht worden genomen.

ii. De beginselen zijn alleen van toepassing wanneer bestanden over individueel geïdentificeerde of identificeerbare personen worden doorgegeven of toegankelijk worden gemaakt. Statistische informatie die berust op geaggregeerde personeelsgegevens en geen persoonsgegevens bevat of het gebruik van geanonimiseerde gegevens, geeft geen aanleiding tot problemen in verband met de bescherming van de privacy.

b. Toepassing van het kennisgevingsbeginsel en het keuzebeginsel

i. Een organisatie in de Verenigde Staten die in het kader van het EU-VS-DPF personeelsgegevens uit de EU heeft ontvangen, mag deze informatie alleen in overeenstemming met het kennisgevingsbeginsel en het keuzebeginsel aan derden bekendmaken of voor andere doeleinden gebruiken. Wanneer een organisatie in de Verenigde Staten bijvoorbeeld van plan is persoonlijke informatie die in het kader van een arbeidsverhouding is verzameld, te gebruiken voor doeleinden die niet met de arbeidsrelatie te maken hebben, zoals commerciële mededelingen, moet zij de betrokkenen vooraf de vereiste keuze laten, tenzij deze al toestemming hadden gegeven om de informatie voor dergelijke doeleinden te gebruiken. Een dergelijk gebruik mag niet onverenigbaar zijn met de doeleinden waarvoor de persoonlijke informatie is verzameld of waarmee de natuurlijke persoon achteraf heeft ingestemd. Bovendien mag de keuze van de werknemers niet van invloed zijn op hun carrièremogelijkheden en mag deze ook geen strafmaatregelen tot gevolg hebben.

ii. Voor sommige EU-lidstaten geldt dat bepaalde algemeen geldende voorwaarden voor doorgifte een ander gebruik van dergelijke informatie uitsluiten, zelfs wanneer de informatie naar een land buiten de EU is doorgegeven. Dergelijke voorwaarden moeten worden nageleefd.

iii. Voorts moeten werkgevers zich redelijkerwijs inspannen om aan de wensen van hun werknemers inzake de bescherming van hun privacy tegemoet te komen. Zij kunnen bijvoorbeeld de toegang tot persoonsgegevens beperken, sommige gegevens anonimiseren of codes of pseudoniemen gebruiken wanneer de echte namen in het onderhavige geval niet nodig zijn voor beleidsdoeleinden.

iv. Voor zover en zolang het noodzakelijk is om te voorkomen dat afbreuk wordt gedaan aan de mogelijkheid van een organisatie om besluiten inzake bevorderingen of benoemingen of andere besluiten ten aanzien van de werknemers te nemen, hoeft een organisatie het kennisgevingsbeginsel en het keuzebeginsel niet toe te passen.

c. Toepassing van het toegangsbeginsel

i. Het aanvullende toegangsbeginsel verschaft richtsnoeren ten aanzien van de redenen op grond waarvan verzoeken om toegang tot personeelsgegevens kunnen worden afgewezen dan wel de toegang tot deze gegevens kan worden beperkt. Het spreekt vanzelf dat werkgevers in de EU er overeenkomstig de wetgeving van hun land voor moeten zorgen dat hun werknemers in de EU toegang hebben tot dergelijke informatie, ongeacht de plaats waar de gegevens worden verwerkt en opgeslagen. Overeenkomstig het EU-VS-DPF moet een organisatie die dergelijke gegevens in de Verenigde Staten verwerkt, deze toegang direct of via de werkgever in de EU verlenen.

d. Handhaving

i. Voor zover persoonlijke informatie alleen in het kader van een arbeidsverhouding wordt gebruikt, ligt de primaire verantwoordelijkheid voor de gegevens ten opzichte van de werknemer bij de organisatie in de EU. Hieruit volgt dat Europese werknemers die over schendingen van hun rechten inzake gegevensbescherming klagen en niet tevreden zijn met de resultaten van interne controle-, klachten- en beroepsprocedures (of elke andere toepasselijke klachtenprocedure in het kader van een overeenkomst met een vakbond), zich moeten wenden tot de bevoegde deelstaat- of nationale gegevensbeschermingsautoriteit of arbeidsrechtbank in het rechtsgebied waar zij werken. Dit geldt ook voor gevallen waarin het beweerde misbruik van de persoonlijke informatie onder de verantwoordelijkheid valt van de organisatie in de Verenigde Staten die de informatie van de werkgever heeft ontvangen. In dergelijke gevallen gaat het dus om een vermeende schending van de beginselen. Dit is de efficiëntste manier om een oplossing te vinden voor de elkaar vaak overlappende rechten en verplichtingen uit hoofde van de lokale arbeidswetgeving en arbeidsovereenkomsten en de wetgeving inzake gegevensbescherming.

ii. Een aan het EU-VS-DPF deelnemende organisatie in de Verenigde Staten die gebruikmaakt van in het kader van een arbeidsverhouding vanuit de EU doorgegeven gegevens over personeel in de EU en die wil dat dergelijke doorgiften onder het EU-VS-DPF vallen, moet zich er dus toe verplichten mee te werken aan onderzoeken van de bevoegde autoriteiten in de EU en hun advies in dergelijke gevallen op te volgen.

e. Toepassing van het beginsel van de aansprakelijkheid voor verdere doorgifte

i. Voor incidentele arbeidsgerelateerde operationele behoeften van de deelnemende organisatie ten aanzien van in het kader van het EU-VS-DPF doorgegeven persoonsgegevens, zoals de boeking van een vlucht of een hotelkamer, of het afsluiten van een verzekering, kan de doorgifte van persoonsgegevens van een klein aantal werknemers aan verwerkingsverantwoordelijken plaatsvinden zonder het toegangsbeginsel toe te passen of een overeenkomst te sluiten met een derde verwerkingsverantwoordelijke, zoals anders vereist is op grond van het beginsel van aansprakelijkheid voor verdere doorgifte, mits de deelnemende organisatie het kennisgevingsbeginsel en het keuzebeginsel in acht heeft genomen.

10. **Verplichte overeenkomsten voor verdere doorgifte**

a. Gegevensverwerkingsovereenkomsten

i. Wanneer persoonsgegevens alleen om ze te laten verwerken uit de EU naar de Verenigde Staten worden doorgegeven, is een overeenkomst vereist, ongeacht of de verwerker aan het EU-VS-DPF deelneemt.

ii. De verwerkingsverantwoordelijken in de EU moeten altijd een overeenkomst sluiten wanneer gegevens alleen voor verwerking worden doorgegeven, ongeacht of dit binnen de EU of daarbuiten gebeurt en ongeacht of de verwerker aan het EU-VS-DPF deelneemt. Het doel van de overeenkomst is ervoor te zorgen dat de verwerker:

1. uitsluitend volgens de instructies van de verwerkingsverantwoordelijke handelt;

2. passende technische en organisatorische veiligheidsmaatregelen treft om persoonsgegevens te beschermen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, verlies, vervalsing of niet-toegelaten verspreiding of toegang, en begrijpt of verdere doorgifte toegelaten is; en

3. rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke bijstaat bij het geven van antwoord aan de natuurlijke personen die hun rechten uit hoofde van de beginselen uitoefenen.

iii. Omdat de deelnemende organisaties passende bescherming bieden, is voor overeenkomsten met dergelijke organisaties voor louter verwerking geen voorafgaande toestemming vereist.

b. Doorgifte binnen een gecontroleerde groep van ondernemingen of entiteiten

i. Wanneer persoonlijke informatie wordt doorgegeven tussen twee verwerkingsverantwoordelijken binnen een gecontroleerde groep van ondernemingen of entiteiten, is een overeenkomst in het kader van het beginsel van aansprakelijkheid voor verdere doorgifte niet altijd nodig. Verwerkingsverantwoordelijken binnen een gecontroleerde groep van ondernemingen of entiteiten kunnen een dergelijke doorgifte baseren op andere instrumenten, zoals bindende EU-bedrijfsvoorschriften of andere intragroepsinstrumenten (bv. nalevings- en controleprogramma's), waarmee de voortzetting van de bescherming van persoonlijke informatie in het kader van de beginselen wordt gegarandeerd. In geval van een dergelijke doorgifte blijft de deelnemende organisatie verantwoordelijk voor de naleving van de beginselen.

c. Doorgifte tussen verwerkingsverantwoordelijken

i. Voor doorgifte tussen verwerkingsverantwoordelijken hoeft de ontvangende verwerkingsverantwoordelijke geen deelnemende organisatie te zijn en niet te beschikken over een onafhankelijk verhaalsmechanisme. De deelnemende organisatie moet een overeenkomst sluiten met de ontvangende derde verwerkingsverantwoordelijke, waarmee dezelfde mate van bescherming wordt geboden als beschikbaar is in het kader van het EU-VS-DPF, en waarbij niet vereist is dat de derde verwerkingsverantwoordelijke een deelnemende organisatie is of beschikt over een onafhankelijk verhaalsmechanisme, mits hij een gelijkwaardig mechanisme ter beschikking stelt.

11. **Geschillenbeslechting en handhaving**

a. Het beginsel van verhaal, handhaving en aansprakelijkheid stelt de eisen vast waaraan handhaving van het EU-VS-DPF moet voldoen. Hoe aan de eisen van punt a), ii) van het beginsel moet worden voldaan, wordt uiteengezet in het aanvullend beginsel inzake controle. Dit aanvullend beginsel heeft betrekking op de punten a), i) en a), iii), die beide onafhankelijke verhaalsmechanismen vereisen. Deze mechanismen kunnen verschillende vormen aannemen, maar moeten voldoen aan de eisen van het beginsel van verhaal, handhaving en aansprakelijkheid. Op de volgende wijze voldoen organisaties aan deze eisen: i) door naleving van programma's van de particuliere sector inzake privacybescherming die de beginselen in hun voorschriften integreren en doeltreffende handhavingsmechanismen omvatten zoals die welke in het beginsel van verhaal, handhaving en aansprakelijkheid worden beschreven; ii) door zich te onderwerpen aan wettelijke of regulerende toezichthoudende autoriteiten die individuele klachten behandelen en geschillen afhandelen; of iii) door zich ertoe te verbinden met de gegevensbeschermingsautoriteiten in de EU of hun gemachtigde vertegenwoordigers samen te werken.

b. Deze lijst is bedoeld ter illustratie en is niet uitputtend. De particuliere sector kan aanvullende handhavingsmechanismen ontwikkelen mits deze aan de eisen van het beginsel van verhaal, handhaving en aansprakelijkheid en de aanvullende beginselen voldoen. De vereisten van het beginsel van verhaal, handhaving en aansprakelijkheid vormen een aanvulling op het vereiste dat zelfreguleringsinspanningen afdwingbaar moeten zijn krachtens sectie 5 van de FTC Act (15 U.S.C. § 45) die oneerlijke of misleidende handelingen verbiedt, 49 U.S. C. § 41712 die een luchtvaartmaatschappij of een reisbureau verbiedt zich in te laten met oneerlijke of misleidende praktijken in het luchtvervoer of de verkoop van luchtvervoer, of een andere wet of regelgeving die dergelijke handelingen verbiedt.

c. Om te bevorderen dat de nakoming van hun toezeggingen in het kader van het EU-VS-DPF wordt gegarandeerd en om het beheer van het programma te ondersteunen, moeten de organisaties, evenals hun onafhankelijke verhaalsmechanismen, informatie over het EU-VS-DPF verstrekken wanneer het ministerie daarom vraagt. Bovendien moeten organisaties snel reageren op klachten over hun naleving van de beginselen die gegevensbeschermingsautoriteiten via het ministerie indienen. In het antwoord moet worden aangegeven of de klacht gegrond is, en zo ja, hoe de organisatie het probleem zal verhelpen. Het ministerie zal de vertrouwelijkheid van de ontvangen informatie beschermen in overeenstemming met de wetgeving van de Verenigde Staten.

d. Verhaalsmechanismen

i. Natuurlijke personen moeten worden aangemoedigd eventuele klachten met de desbetreffende organisatie te bespreken alvorens een beroep te doen op onafhankelijke verhaalsmechanismen. Organisaties moeten een natuurlijke persoon binnen 45 dagen na ontvangst van diens klacht een reactie bezorgen. De onafhankelijkheid van een verhaalsmechanisme kan met name worden aangetoond op grond van onpartijdigheid, een transparante samenstelling en financiering en aantoonbare ervaring. Zoals het beginsel van verhaal, handhaving en aansprakelijkheid vereist, moet het verhaalsmechanisme voor natuurlijke personen direct beschikbaar en kosteloos zijn. Onafhankelijke geschillenbeslechtingsinstanties moeten alle klachten van natuurlijke personen onderzoeken tenzij deze duidelijk ongegrond of onbeduidend zijn. Dit sluit niet uit dat de onafhankelijke geschillenbeslechtingsinstantie waar men verhaal moet halen, acceptatiecriteria vaststelt, maar deze moeten transparant en gerechtvaardigd zijn (bijvoorbeeld om klachten uit te sluiten die buiten het toepassingsgebied van het programma vallen of door een andere instantie moeten worden behandeld) en mogen er niet toe leiden dat de verplichting om gegronde klachten te onderzoeken, wordt ondermijnd. Bovendien moeten verhaalsmechanismen natuurlijke personen die een klacht indienen, complete en direct beschikbare informatie verstrekken over de wijze waarop de procedure verloopt. Deze informatie moet ook betrekking hebben op de door het mechanisme overeenkomstig de beginselen toegepaste praktijken inzake de privacybescherming. Zij moeten ook meewerken bij de ontwikkeling van hulpmiddelen zoals gestandaardiseerde klachtenformulieren om de klachtenafhandelingsprocedure te vergemakkelijken.

ii. Onafhankelijke verhaalsmechanismen moeten op hun openbare websites informatie opnemen over de beginselen en over de diensten die zij in het kader van het EU-VS-DPF aanbieden. Deze informatie moet het volgende bevatten: 1) informatie over of een link naar de vereisten van de beginselen voor onafhankelijke verhaalsmechanismen; 2) een link naar de DPF-website van het ministerie; 3) een toelichting dat hun diensten inzake geschillenbeslechting in het kader van het EU-VS-DPF voor natuurlijke personen kosteloos zijn; 4) een beschrijving van de wijze waarop een klacht in verband met de beginselen kan worden ingediend; 5) de termijnen waarbinnen klachten inzake de beginselen worden behandeld; en 6) een beschrijving van het scala aan verhaalsmogelijkheden.

iii. Onafhankelijke verhaalsmechanismen moeten een jaarverslag publiceren met geaggregeerde statistieken over hun geschillenbeslechtingsdiensten. Het jaarverslag moet het volgende bevatten: 1) het totale aantal tijdens het verslagjaar ontvangen klachten in verband met de beginselen; 2) de soorten ontvangen klachten; 3) maatstaven inzake de kwaliteit van de geschillenbeslechting, zoals de tijd die met de verwerking van klachten gemoeid was; en 4) de resultaten van de ontvangen klachten, met name het aantal en de soorten genomen maatregelen of opgelegde sancties.

iv. Zoals uiteengezet in bijlage I beschikken natuurlijke personen over een arbitrage-optie teneinde ten aanzien van resterende klachten te bepalen of een deelnemende organisatie haar verplichtingen in het kader van de beginselen tegenover hen heeft geschonden, en of een dergelijke schending in het geheel niet of maar gedeeltelijk werd verholpen. Deze optie is alleen beschikbaar voor deze doeleinden. Deze optie is bijvoorbeeld niet beschikbaar met betrekking tot de uitzonderingen op de beginselen ([15]) of met betrekking tot een bewering over het passend karakter van het EU-VS-DPF. In het kader van deze arbitrage-optie is het "panel van het EU-VS-kader voor gegevensbescherming" (bestaande uit één of drie arbiters, zoals overeengekomen door de partijen) bevoegd om een individuele, specifieke, niet-geldelijke, billijke voorziening vast te stellen (zoals toegang, correctie, wissing of teruggave van de betrokken gegevens van de natuurlijke persoon) die nodig is om de schending van de beginselen in verband met enkel deze natuurlijke persoon te verhelpen. Natuurlijke personen en deelnemende organisaties kunnen op grond van de Federal Arbitration Act de rechterlijke toetsing en tenuitvoerlegging van de arbitragebeslissingen vorderen krachtens Amerikaans recht.

e. Rechtsmiddelen en sancties

i. De rechtsmiddelen die de onafhankelijke geschillenbeslechtingsinstantie biedt, moeten ertoe leiden dat de gevolgen van de niet-naleving door de organisatie, voor zover mogelijk, ongedaan worden gemaakt of worden hersteld, dat de organisatie gegevens in de toekomst conform de beginselen zal verwerken en dat, waar nodig, de verwerking van de persoonsgegevens van de klager wordt stopgezet. De sancties moeten zwaar genoeg zijn om de naleving van de beginselen door de organisatie te waarborgen. Aan de hand van een scala van lichte tot zware sancties zullen geschillenbeslechtingsinstanties op passende wijze kunnen reageren op in ernst variërende gevallen van niet-naleving. Tot de sancties moeten behoren: bekendmaking

([15]) De beginselen, overzicht, punt 5.

van geconstateerde gevallen van niet-naleving en de eis gegevens in bepaalde omstandigheden te wissen ([16]). Andere mogelijke sancties zijn de opschorting en intrekking van een keurmerk, schadeloosstelling van personen voor verliezen die ze als gevolg van niet-naleving hebben geleden, en dwangmaatregelen. Particuliere onafhankelijke geschillenbeslechtingsinstanties en zelfregulerende instanties moeten in voorkomend geval de rechter of de ter zake bevoegde overheidsinstantie in kennis stellen van de niet-inachtneming van hun uitspraken door deelnemende organisaties, en het ministerie daarvan op de hoogte stellen.

f. Actie van de FTC

i. De FTC zal prioriteit geven aan zaken die haar in verband met de niet-naleving van de beginselen worden voorgelegd door: i) zelfregulerende instanties voor privacybescherming en andere onafhankelijke geschillenbeslechtingsinstanties; ii) de EU-lidstaten; en iii) het ministerie, om na te gaan of er sprake is van schending van sectie 5 van de FTC Act, die oneerlijke of misleidende handelspraktijken verbiedt. Indien de FTC concludeert dat zij reden heeft om aan te nemen dat sectie 5 werd geschonden, kan zij de zaak oplossen door om een administratief verbod van de bestreden praktijken te verzoeken, of door bij een federale rechtbank een klacht in te dienen, die als zij wordt gehonoreerd, kan resulteren in een uitspraak die hetzelfde effect sorteert. Daarbij kan het gaan om valse verklaringen inzake de onderschrijving van de beginselen of deelname aan het EU-VS-DPF door organisaties die ofwel niet meer op de DPF-lijst staan ofwel nooit bij het ministerie een zelfcertificeringsverklaring hebben ingediend. De FTC kan civielrechtelijk optreden wegens overtreding van een administratief verbod, dan wel civiel- of strafrechtelijk wegens niet-naleving van een uitspraak van een federale rechtbank. De FTC zal het ministerie van dergelijke acties in kennis stellen. Het ministerie moedigt andere overheidsinstanties ertoe aan het uiteindelijke resultaat van dergelijke verwijzingen of andere uitspraken in verband met de naleving van de beginselen aan het ministerie mee te delen.

g. Permanente niet-naleving

i. Als een organisatie voortdurend de beginselen overtreedt, komt ze niet langer in aanmerking voor de voordelen van het EU-VS-DPF. Een organisatie zal in geval van permanente niet-naleving van de beginselen door het ministerie van de DPF-lijst worden verwijderd en de in het kader van het EU-VS-DPF ontvangen persoonsgegevens moeten terugbezorgen of wissen.

ii. Er is sprake van permanente niet-naleving indien een organisatie die bij het ministerie een zelfcertificeringsverklaring heeft ingediend, weigert zich te conformeren aan een definitieve uitspraak van een zelfregulerende, onafhankelijke geschillenbeslechtingsinstantie op het gebied van de privacy of van een overheidsinstantie of indien een dergelijke instantie, met inbegrip van het ministerie, constateert dat een organisatie zich vaak niet aan de beginselen houdt en haar verklaring deze te zullen naleven niet langer geloofwaardig is. Indien een dergelijke vaststelling wordt gedaan door een andere instantie dan het ministerie moet de organisatie het ministerie onverwijld van deze feiten in kennis stellen. Als zij dit niet doet, kan op grond van de False Statements Act (18 U.S.C. § 1001) vervolging tegen deze organisatie worden ingesteld. Wanneer een organisatie zich terugtrekt uit een particulier zelfreguleringsprogramma op het gebied van privacy of een onafhankelijk geschillenbeslechtingsmechanisme, ontslaat dat de organisatie niet van de verplichting om de beginselen na te leven en kan van een permanente niet-naleving sprake zijn.

iii. Het ministerie zal een organisatie van de DPF-lijst schrappen wegens permanente niet-naleving, ook naar aanleiding van een kennisgeving die het ontvangt van de organisatie zelf, van een zelfregulerende instantie voor privacy of een andere onafhankelijke geschillenbeslechtingsinstantie, of van een overheidsinstantie, maar pas nadat de organisatie 30 dagen van tevoren in kennis is gesteld en de gelegenheid heeft gekregen te reageren ([17]). Uit deze door het ministerie bijgehouden DPF-lijst blijkt derhalve welke organisaties verder voor de voordelen van het EU-VS-DPF in aanmerking komen en welke niet.

iv. Een organisatie die zich bij een zelfregulerende instantie aansluit om opnieuw voor het EU-VS-DPF in aanmerking te komen, moet deze instantie volledige informatie over haar vroegere deelneming aan het EU-VS-DPF verstrekken.

([16]) Onafhankelijke geschillenbeslechtingsinstanties moeten een discretionaire bevoegdheid hebben ten aanzien van de omstandigheden waarin zij deze sancties opleggen. Bij een eis gegevens te wissen moet onder meer rekening worden gehouden met de gevoeligheid van de gegevens en met het feit of een organisatie flagrant in strijd met de beginselen gegevens heeft verzameld of gebruikt, dan wel openbaar heeft gemaakt.

([17]) Het ministerie zal in de kennisgeving aangeven hoeveel tijd, die noodzakelijkerwijs minder dan 30 dagen zal bedragen, de organisatie heeft om op de kennisgeving te reageren.

12. **Keuze — Tijdstip van verzet (opt-out)**

a. Het keuzebeginsel heeft als doel ervoor te zorgen dat persoonlijke informatie wordt gebruikt en bekend wordt gemaakt op een manier die tegemoetkomt aan de verwachtingen en de keuzes van de natuurlijke persoon. Daarom moet deze te allen tijde de mogelijkheid hebben zich tegen het gebruik van zijn persoonlijke informatie voor directe marketing te verzetten; hij moet dit wel doen binnen door de organisatie vastgestelde, redelijke termijnen, zodat de organisatie de tijd heeft gevolg aan de keuze te geven. Een organisatie kan ook eisen dat haar voldoende informatie wordt verstrekt ter bevestiging van de identiteit van de natuurlijke persoon die zich verzet. In de Verenigde Staten kunnen natuurlijke personen dit recht uitoefenen via een centraal verzetprogramma. In ieder geval moet de natuurlijke persoon een beroep kunnen doen op een direct beschikbaar en betaalbaar mechanisme om dit keuzerecht uit te oefenen.

b. Een organisatie kan ook informatie voor sommige direct-marketingactiviteiten gebruiken wanneer het praktisch onmogelijk is om de natuurlijke persoon de gelegenheid te geven verzet aan te tekenen voordat de informatie wordt gebruikt, op voorwaarde dat de organisatie de natuurlijke persoon meteen daarna (en op verzoek altijd) de mogelijkheid biedt om verdere ontvangst van direct-marketingmededelingen te weigeren (zonder dat dit voor de natuurlijke persoon kosten met zich brengt) en op voorwaarde dat de organisatie tegemoetkomt aan de wensen van de natuurlijke persoon.

13. **Reisinformatie**

a. Informatie over boekingen van luchtvaartpassagiers en andere reisinformatie, bijvoorbeeld over bonusregelingen voor vaste klanten of hotelreserveringen, en speciale behandelingen, zoals aan religieuze vereisten aangepaste maaltijden of fysieke bijstand, mogen in een aantal verschillende omstandigheden aan organisaties buiten de EU worden doorgegeven. Krachtens de AVG kunnen persoonsgegevens, bij ontstentenis van een adequaatheidsbesluit, worden doorgegeven aan een derde land indien er overeenkomstig artikel 46 AVG passende gegevensbeschermingswaarborgen worden geboden of, in specifieke situaties, indien aan een van de voorwaarden van artikel 49 AVG is voldaan (bijvoorbeeld wanneer de betrokkene uitdrukkelijk met de doorgifte heeft ingestemd). Amerikaanse organisaties die het EU-VS-DPF onderschrijven, bieden een passende bescherming voor persoonsgegevens en kunnen derhalve gegevensdoorgiften uit de EU ontvangen op basis van artikel 45 AVG, zonder dat zij een doorgifte-instrument overeenkomstig artikel 46 AVG hoeven in te stellen of aan de voorwaarden van artikel 49 AVG hoeven te voldoen. Aangezien het EU-VS-DPF specifieke regels voor gevoelige informatie omvat, kan dergelijke informatie (die soms moet worden verzameld, bijvoorbeeld omdat een passagier fysieke bijstand nodig heeft) aan deelnemende organisaties worden doorgegeven. In alle gevallen moet de organisatie die de informatie doorgeeft, zich echter houden aan de wet van de EU-lidstaat waar zij actief is; deze kan onder meer bijzondere voorwaarden aan de behandeling van gevoelige gegevens stellen.

14. **Farmaceutische en medische producten**

a. Toepassing van de wetgeving van de EU-lidstaten of de beginselen

i. De wetgeving van de EU-lidstaten is van toepassing op de verzameling van de persoonsgegevens, alsmede op de verwerking voor zover die plaatsvindt vóór de doorgifte aan de Verenigde Staten. De beginselen zijn op de gegevens van toepassing vanaf het moment dat zij naar de Verenigde Staten zijn doorgegeven. Gegevens die voor farmaceutisch onderzoek en andere doeleinden worden gebruikt, moeten indien nodig worden geanonimiseerd.

b. Later wetenschappelijk onderzoek

i. Persoonsgegevens uit specifiek medisch of farmaceutisch onderzoek spelen veelal een belangrijke rol bij later wetenschappelijk onderzoek. Als de voor een bepaald onderzoek verzamelde persoonsgegevens worden doorgegeven aan een organisatie in de Verenigde Staten die aan het EU-VS-DPF deelneemt, mag de organisatie de gegevens gebruiken voor nieuw wetenschappelijk onderzoek, mits de betrokkene hiervan in eerste instantie op de juiste wijze in kennis was gesteld en hij een keuzemogelijkheid had. Deze kennisgeving moet informatie bevatten over ieder specifiek gebruik van de gegevens in de toekomst, zoals periodieke follow-up, verwante studies of verkoopactiviteiten.

ii. Het spreekt voor zich dat niet ieder toekomstig gebruik van de gegevens kan worden voorzien, aangezien het nieuwe onderzoek waarvoor de gegevens zullen worden gebruikt, kan voortvloeien uit op grond van de oorspronkelijke gegevens verworven nieuwe inzichten, nieuwe medische ontdekkingen en vorderingen en de ontwikkeling van de volksgezondheid en regelgeving. In voorkomende gevallen moet de kennisgeving dan ook een toelichting bevatten waarin is aangegeven dat de persoonsgegevens voor toekomstig, nog niet te voorzien medisch en farmaceutisch onderzoek kunnen worden gebruikt. Als dit gebruik afwijkt van de algemene onderzoeksdoelstelling(en) waarvoor de persoonsgegevens oorspronkelijk zijn verzameld of waarvoor de natuurlijke persoon later toestemming heeft gegeven, is opnieuw toestemming vereist.

c. Opzegging van medewerking aan een klinische proef

i. Deelnemers kunnen op ieder moment hun medewerking aan een klinische proef opzeggen, of hiertoe worden verzocht. Alle persoonsgegevens die voorafgaand aan deze terugtrekking zijn verzameld, mogen toch, samen met de overige verzamelde gegevens, in de klinische proef worden verwerkt, mits de deelnemer hiervan op het moment dat hij in deelname toestemde, in kennis is gesteld.

d. Overdrachten met het oog op regelgeving en toezicht

i. Producenten van geneesmiddelen en medische apparatuur mogen persoonsgegevens uit in de EU uitgevoerde klinische proeven met het oog op regelgeving en toezicht doorgeven aan instanties in de Verenigde Staten. Een soortgelijke doorgifte is ook toegestaan aan andere partijen dan regelgevende instanties, zoals bedrijfsvestigingen en andere onderzoekers, mits dit in overeenstemming is met het kennisgevingsbeginsel en het keuzebeginsel.

e. "Blinde" tests

i. Met het oog op de objectiviteit mogen deelnemers, en vaak ook onderzoekers, bij veel klinische proeven niet weten welke behandeling iedere deelnemer ondergaat. Als dit wel het geval was, zouden de validiteit van het onderzoek en de resultaten in gevaar komen. Deelnemers aan dergelijke klinische proeven (aangeduid als "blinde" tests) hoeven tijdens de proef geen toegang te krijgen tot de gegevens over hun behandeling indien deze beperking is aangegeven toen de deelnemer toestemde in deelname aan de proef en bekendmaking van dergelijke informatie de validiteit van het onderzoek in gevaar brengt.

ii. Toestemming in deelname aan de proef onder deze voorwaarden geldt als het afzien van het recht op toegang tot deze informatie. Na de voltooiing van de proef en de analyse van de resultaten moeten de deelnemers desgewenst toegang tot hun gegevens krijgen. Zij moeten zich hiervoor in eerste instantie wenden tot de arts of andere zorgverstrekker door wie zij in het kader van de medische proef zijn behandeld en in tweede instantie tot de opdrachtgever van de proef.

f. Toezicht op productveiligheid en efficiëntie

i. Producenten van geneesmiddelen en medische apparatuur hoeven de beginselen niet toe te passen met betrekking tot de beginselen van kennisgeving, keuze, aansprakelijkheid voor verdere doorgifte en toegang, wanneer zij maatregelen in verband met de controle op de veiligheid en doeltreffendheid van hun producten nemen, zoals rapportage van incidenten en het volgen van patiënten/proefpersonen die bepaalde geneesmiddelen of medische apparatuur gebruiken, voor zover de naleving van de beginselen samenvalt met de naleving van de wettelijke voorschriften. Dit geldt zowel voor de rapportage door bijvoorbeeld zorgverstrekkers aan producenten van geneesmiddelen en medische apparatuur als voor de rapportage door producenten van geneesmiddelen en medische apparatuur aan overheidsinstanties, zoals de Food and Drug Administration.

g. Gegevens met een unieke code

i. De hoofdonderzoeker voorziet de onderzoeksgegevens altijd al bij de bron van een unieke code, zodat de identiteit van de betrokkenen waarop de gegevens betrekking hebben geheim blijft. De farmaceutische bedrijven die de opdracht voor het onderzoek hebben gegeven, krijgen niet de beschikking over de sleutel. Deze is uitsluitend bij de onderzoeker bekend, zodat hij onder bepaalde omstandigheden (bv. als achteraf nog medische zorg nodig is) de betrokkene kan identificeren. Een doorgifte van de EU naar de Verenigde Staten van aldus gecodeerde gegevens die volgens het EU-recht persoonsgegevens zijn, zou onder de beginselen vallen.

15. **Informatie uit openbare bestanden of openbaar beschikbare informatie**

a. Een organisatie moet de beginselen van veiligheid, de integriteit van gegevens en doelbinding en verhaal, handhaving en aansprakelijkheid toepassen op persoonsgegevens uit openbare bronnen. Deze beginselen gelden ook voor persoonsgegevens die worden verzameld uit openbare bestanden (d.w.z. bestanden die door overheidsdiensten op alle mogelijke niveaus worden bewaard en die voor iedereen toegankelijk zijn).

b. Het is niet nodig de beginselen van kennisgeving, keuze of aansprakelijkheid voor verdere doorgifte toe te passen op informatie uit openbare bestanden, op voorwaarde dat deze informatie niet is gecombineerd met informatie uit niet-openbare bestanden en alle voorwaarden die de bevoegde instanties voor raadpleging stellen, worden nageleefd. In het algemeen is het evenmin nodig de beginselen van kennisgeving, keuze of aansprakelijkheid voor verdere doorgifte toe te passen op openbaar beschikbare informatie, tenzij de Europese organisatie die de informatie doorgeeft, aangeeft dat voor deze informatie beperkingen gelden, op grond waarvan die beginselen in verband met het gebruik dat zij van de informatie wil maken door de organisatie moeten worden toegepast. Organisaties zijn niet aansprakelijk voor de manier waarop dergelijke informatie wordt gebruikt door degenen die de informatie uit gepubliceerd materiaal hebben verkregen.

c. Indien wordt geconstateerd dat een organisatie persoonlijke informatie opzettelijk in strijd met de beginselen openbaar heeft gemaakt, zodat zij of anderen van deze uitzonderingen kunnen profiteren, komt zij niet langer voor het EU-VS-DPF in aanmerking.

d. Het is niet nodig het toegangsbeginsel op informatie uit openbare bestanden toe te passen, voor zover deze niet wordt gecombineerd met andere persoonlijke informatie (tenzij het hierbij gaat om kleine hoeveelheden die worden gebruikt om informatie uit openbare bestanden te indexeren of te organiseren); de voorwaarden die de bevoegde instanties voor raadpleging stellen, moeten evenwel worden nageleefd. Wanneer daarentegen informatie uit openbare bestanden wordt gecombineerd met andere informatie uit niet-openbare bestanden (afgezien van bovengenoemd specifiek geval), dan moet een organisatie wel toegang tot al deze informatie verlenen, voor zover niet andere toegestane uitzonderingen op deze informatie van toepassing zijn.

e. Net als voor informatie uit openbare bestanden is het niet nodig toegang te verlenen tot informatie die reeds voor iedereen beschikbaar is, voor zover deze niet wordt gecombineerd met niet-openbaar beschikbare informatie. Organisaties die openbaar beschikbare informatie verkopen, kunnen het voor hun organisatie gebruikelijke tarief in rekening brengen om aan de verzoeken tot toegang te voldoen. Natuurlijke personen kunnen echter ook toegang tot hun persoonsgegevens trachten te verkrijgen bij de organisatie die oorspronkelijk de gegevens heeft verzameld.

16. **Verzoeken om toegang door de overheid**

a. Met het oog op de transparantie inzake gerechtvaardigde verzoeken van openbare instanties om toegang tot persoonlijke informatie, kunnen deelnemende organisaties op vrijwillige basis periodieke transparantie-verslagen uitbrengen inzake het aantal verzoeken om persoonlijke informatie die zij van openbare instanties ontvangen om redenen van rechtshandhaving of nationale veiligheid, voor zover dergelijke bekendmakingen overeenkomstig het toepasselijke recht toegestaan zijn.

b. De door de deelnemende organisaties in deze verslagen verstrekte informatie kan samen met de informatie die werd vrijgegeven door inlichtingendiensten, alsook andere informatie, worden gebruikt ten behoeve van de periodieke gezamenlijke evaluatie van de werking van het EU-VS-DPF overeenkomstig de beginselen.

c. Het ontbreken van een kennisgeving overeenkomstig punt a), xii), van het kennisgevingsbeginsel mag de mogelijkheid voor een organisatie om te reageren op een gerechtvaardigd verzoek niet verhinderen of beperken.

BIJLAGE I: ARBITRAGEMODEL

In deze bijlage I wordt beschreven wanneer organisaties die deelnemen aan het EU-VS-DPF verplicht zijn klachten op grond van het beginsel van verhaal, handhaving en aansprakelijkheid aan arbitrage te onderwerpen. De hieronder omschreven bindende arbitrage-optie geldt voor bepaalde "resterende" klachten in verband met gegevens die onder het EU-VS-DPF vallen. Het doel van deze optie is een snel, onafhankelijk en eerlijk mechanisme te bieden, waarvan de natuurlijke personen desgewenst gebruik kunnen maken in geval van een geschil over schendingen van de beginselen dat niet via een van de andere EU-VS-DPF-mechanismen werd beslecht.

A. **Toepassingsgebied**

Deze arbitrage-optie staat ter beschikking van natuurlijke personen en maakt het mogelijk om ten aanzien van nog niet anderszins opgeloste klachten te bepalen of een deelnemende organisatie haar verplichtingen in het kader van de beginselen tegenover iemand heeft geschonden, en of een dergelijke schending volledig of gedeeltelijk niet werd verholpen. Deze optie is alleen beschikbaar voor deze doeleinden. Deze optie is bijvoorbeeld niet beschikbaar met betrekking tot de uitzonderingen op de beginselen ([1]) of met betrekking tot een bewering over het passend karakter van het EU-VS-DPF.

B. **Beschikbare verhaalsmiddelen**

In het kader van deze arbitrage-optie is het "panel van het EU-VS-kader voor gegevensbescherming" (bestaande uit één of drie arbiters, zoals overeengekomen door de partijen) bevoegd om een individuele, specifieke, niet-geldelijke, billijke voorziening vast te stellen (zoals toegang, correctie, wissing of teruggave van de betrokken gegevens van de natuurlijke persoon) die nodig is om de schending van de beginselen in verband met enkel deze natuurlijke persoon te verhelpen. Dit zijn de enige bevoegdheden van het panel van het EU-VS-kader voor gegevensbescherming qua voorzieningen. Bij het overwegen van voorzieningen moet het panel van het EU-VS-kader voor gegevensbescherming voorzieningen in overweging nemen die reeds door andere mechanismen werden vastgesteld in het kader van het EU-VS-DPF. Schadevergoeding of vergoeding van kosten of honoraria of andere voorzieningen zijn niet mogelijk. Elke partij betaalt de honoraria van haar eigen advocaat.

C. **Aan arbitrage voorafgaande vereisten**

Een natuurlijke persoon die beslist een beroep te doen op deze arbitrage-optie, moet alvorens een arbitrageverzoek te doen, de volgende stappen ondernemen: 1) rechtstreeks bij de organisatie bezwaar maken tegen de beweerde schending en de organisatie de gelegenheid bieden om de kwestie binnen de in hoofdstuk d), punt i), van het aanvullend beginsel inzake geschillenbeslechting en handhaving bepaalde termijn op te lossen; 2) gebruikmaken van het onafhankelijk verhaalsmechanisme in het kader van de beginselen, dat voor de betrokken persoon gratis is; en 3) de zaak via de gegevensbeschermingsautoriteit van de natuurlijke persoon aankaarten bij het ministerie en het ministerie de mogelijkheid bieden zijn uiterste best te doen om het probleem op de lossen binnen de termijnen waarin is voorzien in de brief van de International Trade Administration van het ministerie. Hieraan zijn voor de betrokken persoon geen kosten verbonden.

Deze arbitrage-optie kan niet worden ingeroepen indien de beweerde schending van de beginselen 1) reeds eerder was onderworpen aan bindende arbitrage; 2) het voorwerp uitmaakt van een onherroepelijk vonnis dat is gegeven in het kader van een gerechtelijke procedure waarbij de natuurlijke persoon partij was; of 3) reeds eerder door de partijen werd geregeld. Bovendien kan deze optie niet worden ingeroepen indien een gegevensbeschermingsautoriteit 1) bevoegd is krachtens het aanvullend beginsel inzake de rol van de gegevensbeschermingsautoriteiten of het aanvullend beginsel inzake personeelsgegevens; of 2) de bevoegdheid heeft om de beweerde overtreding rechtstreeks met de organisatie op te lossen. De bevoegdheid van een gegevensbeschermingsautoriteit om een klacht jegens een EU-verwerkingsverantwoordelijke af te handelen, sluit op zich niet de mogelijkheid uit om inzake dezelfde klacht van deze arbitrage-optie gebruik te maken jegens een andere juridische entiteit waarover de gegevensbeschermingsautoriteit geen bevoegdheid heeft.

D. **Bindend karakter van beslissingen**

De beslissing van een natuurlijke persoon om deze bindende arbitrage-optie in te roepen, is volledig vrijwillig. Arbitragebeslissingen zijn bindend voor alle partijen bij de arbitrage. Wanneer de natuurlijke persoon deze optie eenmaal heeft ingeroepen, doet hij afstand van de mogelijkheid om de zaak aan een ander forum voor te leggen, zij het dat wanneer de niet-geldelijke, billijke schadevergoeding de beweerde schending niet volledig vergoedt, de keuze voor de arbitrage de natuurlijke persoon niet belet om eventueel bij de rechter een vordering tot schadevergoeding in te stellen.

([1]) De beginselen, overzicht, punt 5.

E. **Rechterlijke toetsing en tenuitvoerlegging**

Natuurlijke personen en deelnemende organisaties kunnen op grond van de Federal Arbitration Act de rechterlijke toetsing en tenuitvoerlegging van de arbitragebeslissingen vorderen krachtens Amerikaans recht ([2]). In dergelijke gevallen moet een zaak worden ingeleid bij de *federal district court* die bevoegd is met betrekking tot de hoofdzetel van de deelnemende organisatie.

Deze arbitrage-optie beoogt individuele geschillen te beslechten; het is niet de bedoeling dat arbitragebesluiten fungeren als een overtuigend of bindend precedent in zaken waarbij andere partijen betrokken zijn, met inbegrip van toekomstige arbitrages of in procedures voor rechters in de EU of de VS, of FTC-procedures.

F. **Het arbitragepanel**

De partijen kiezen arbiters voor het panel van het EU-VS-kader voor gegevensbescherming uit de hieronder besproken lijst van arbiters.

In overeenstemming met het toepasselijke recht zullen het ministerie en de Commissie een lijst opstellen van ten minste tien arbiters, geselecteerd op basis van onafhankelijkheid, integriteit en expertise. Het volgende is van toepassing in het kader van deze procedure:

Arbiters:

1) blijven op de lijst staan voor een periode van drie jaar, behoudens uitzonderlijke omstandigheden of verwijdering om dringende redenen, die door het ministerie, met voorafgaande kennisgeving aan de Commissie, met drie jaar kan worden verlengd;

2) zijn niet onderworpen aan enige instructie van, of gelieerd aan een partij, of een deelnemende organisatie, of de VS, EU, of een EU-lidstaat of een andere regeringsinstantie, overheidsinstantie, of handhavingsautoriteit; en

3) moeten een vergunning hebben tot uitoefening van de advocatuur in de Verenigde Staten, deskundig zijn op het gebied van de Amerikaanse wetgeving inzake privacybescherming en deskundigheid hebben op het gebied van de EU-wetgeving inzake gegevensbescherming.

([2]) Hoofdstuk 2 van de Federal Arbitration Act ("FAA") bepaalt dat "[e]en arbitrageovereenkomst of arbitrale uitspraak voortvloeiende uit een rechtsverhouding, al dan niet contractueel, die wordt beschouwd als een commerciële verhouding, met inbegrip van een schikking, overeenkomst of afspraak zoals beschreven in [sectie 2 van de FAA], valt onder het Verdrag [van 10 juni 1958 over de erkenning en tenuitvoerlegging van buitenlandse scheidsrechterlijke uitspraken, 21 U.S.T. 2519, T.I.A.S. Nr. 6997 ("Verdrag van New York")]." 9 U.S.C. § 202. De FAA bepaalt voorts dat "[e]en overeenkomst of uitspraak die voortvloeit uit een dergelijke verhouding waarbij alleen de burgers van de Verenigde Staten zijn betrokken, geacht wordt niet onder het Verdrag [van New York] te vallen, tenzij deze verhouding betrekking heeft op in het buitenland gelegen eigendommen, uitvoering of tenuitvoerlegging in het buitenland beoogt, of een andere redelijke band met een of meer buitenlandse staten heeft." 9 U.S.C. § 202. Krachtens hoofdstuk 2 kan "elke partij bij de arbitrage een krachtens dit hoofdstuk bevoegd gerecht verzoeken om een bevel tot bekrachtiging van de uitspraak ten aanzien van elke andere partij bij de arbitrage. De rechter bevestigt de uitspraak, tenzij hij een van de in het [Verdrag van New York] genoemde gronden voor weigering of opschorting van de erkenning of tenuitvoerlegging van de uitspraak vaststelt." 9 U.S.C. § 207. Hoofdstuk 2 bepaalt voorts het volgende: "De *district courts* van de Verenigde Staten […] hebben oorspronkelijke bevoegdheid ten aanzien van […] een beroep of vordering [krachtens het Verdrag van New York], ongeacht het bedrag in geschil." 9 U.S.C. § 203.
In Hoofdstuk 2 is ook bepaald: "Hoofdstuk 1 is […] van toepassing op beroepen die in het kader van dit hoofdstuk worden ingesteld, voor zover dat hoofdstuk niet in strijd is met dit hoofdstuk of met het Verdrag [van New York], zoals geratificeerd door de Verenigde Staten." 9 U.S.C. § 208. Hoofdstuk 1 bepaalt vervolgens dat "[een] schriftelijke bepaling in […] een overeenkomst inzake een commerciële transactie dat een geschil dat daarna rijst op grond van een dergelijke overeenkomst of transactie, of van de weigering om deze in zijn geheel of gedeeltelijk uit te voeren, of een schriftelijke overeenkomst om een bestaand geschil dat voortvloeit uit een dergelijk contract, dergelijke transactie of weigering aan arbitrage te onderwerpen, […] geldig, onherroepelijk en afdwingbaar [is], tenzij er op grond van het recht of de billijkheid redenen zijn om een overeenkomst te herroepen." 9 U.S.C. § 2. Hoofdstuk 1 bepaalt voorts dat "een partij bij de arbitrage deze rechtbank ook [mag] verzoeken om een beschikking tot bevestiging van de beslissing; daarop moet de rechtbank een dergelijke beschikking geven, tenzij de beslissing werd nietig verklaard, gewijzigd of gecorrigeerd zoals voorgeschreven in de secties 10 en 11 van [de FAA]." 9 U.S.C. § 9.

G. **Arbitrageprocedures**

Het ministerie en de Commissie hebben, in overeenstemming met de toepasselijke wetgeving, ingestemd met de vaststelling van arbitrageregels voor de procedures voor het panel van het EU-VS-kader voor gegevensbescherming ([3]). Indien de procedureregels moeten worden gewijzigd, zullen het ministerie en de Commissie overeenkomen deze regels te wijzigen of een andere reeks bestaande, gevestigde arbitrageprocedures van de VS aan te nemen, naargelang van het geval, met inachtneming van elk van de volgende overwegingen:

1. Een natuurlijk persoon kan tot bindende arbitrage overgaan, met inachtneming van de bovenvermelde bepaling inzake aan de arbitrage voorafgaande vereisten, via afgifte van een "kennisgeving" aan de organisatie. De kennisgeving bevat een samenvatting van de stappen die zijn genomen op grond van punt C om de klacht op te lossen, een beschrijving van de beweerde schending en, naar keuze van de natuurlijke persoon, de bewijsstukken en de documenten en/of een uiteenzetting van de wetgeving met betrekking tot de klacht.

2. Er zullen procedures worden ontwikkeld om ervoor te zorgen dat één en dezelfde beweerde schending niet meermaals wordt verholpen of behandeld.

3. FTC-maatregelen kunnen parallel met arbitrage worden genomen.

4. Vertegenwoordigers van de VS, de EU, een EU-lidstaat of een andere regeringsinstantie, overheidsinstantie, of handhavingsautoriteit mogen niet deelnemen aan deze arbitrages, zij het dat gegevensbeschermingsautoriteiten op verzoek van een natuurlijke persoon uit de EU bijstand mogen verlenen bij de voorbereiding van enkel de kennisgeving, zonder echter toegang te hebben tot bekendmakings- of andere documenten met betrekking tot deze arbitrages.

5. De arbitrage zal plaatsvinden in de Verenigde Staten en de betrokken persoon kan opteren voor deelname per video of telefoon, zonder dat voor die persoon aan die deelname kosten zijn verbonden. Fysieke aanwezigheid wordt niet vereist.

6. De arbitrage vindt plaats in de Engelse taal, tenzij door partijen anders is overeengekomen. Op gemotiveerd verzoek, en in aanmerking nemend of de natuurlijke persoon door een advocaat wordt vertegenwoordigd, zal tijdens de arbitragezitting ten behoeve van de natuurlijke persoon voor kosteloze vertolking en kosteloze vertaling van de abitragestukken worden gezorgd, tenzij het panel van het EU-VS-kader voor gegevensbescherming van oordeel is dat dit gelet op de specifieke omstandigheden van de arbitrage in kwestie zou leiden tot ongerechtvaardigde of buitensporige kosten.

7. Stukken die aan de arbiters worden voorgelegd, moeten vertrouwelijk worden behandeld en mogen alleen worden gebruikt in het kader van de arbitrage.

8. Individuele specifieke openbaarmaking kan worden toegestaan indien nodig, en een dergelijke openbaarmaking moet vertrouwelijk worden behandeld door de partijen en mag alleen worden gebruikt in verband met de arbitrage.

9. Arbitrages moeten worden voltooid binnen 90 dagen na de afgifte van de kennisgeving aan de betrokken organisatie, tenzij door de partijen anders overeengekomen is.

([3]) Het International Centre for Dispute Resolution ("ICDR"), de internationale afdeling van de American Arbitration Association ("AAA") (tezamen "ICDR-AAA"), is door het ministerie geselecteerd om de arbitrages te beheren overeenkomstig bijlage I bij de beginselen. Op 15 september 2017 hebben het ministerie en de Commissie ingestemd met de vaststelling van een reeks arbitrageregels voor bindende arbitrageprocedures zoals beschreven in bijlage I bij de beginselen, alsmede een gedragscode voor arbiters die in overeenstemming is met algemeen aanvaarde ethische normen voor commerciële arbiters en bijlage I bij de beginselen. Het ministerie en de Commissie zijn overeengekomen de arbitrageregels en de gedragscode aan te passen aan de updates in het kader van het EU-VS-DPF, en het ministerie zal met het ICDR-AAA samenwerken om deze aanpassingen uit te voeren.

H. **Kosten**

Arbiters moeten redelijke maatregelen treffen om de kosten of vergoedingen inzake de arbitrages zo laag mogelijk te houden.

Overeenkomstig het toepasselijke recht zal het ministerie de oprichting van een fonds bevorderen waaraan de deelnemende organisaties een jaarlijkse bijdrage zullen moeten betalen, welke deels gebaseerd is op de omvang van de organisatie, om de kosten van de arbitrage, inclusief de honoraria van de arbiters, te dekken, ten belope van maximumbedragen ("caps"). Het fonds zal worden beheerd door een derde partij, die regelmatig aan het ministerie verslag uitbrengt over de werkzaamheden van het fonds. Het ministerie zal samenwerken met een derde partij om de werking van het fonds periodiek te evalueren, inclusief de vraag of het bedrag van de bijdragen of van de caps op de arbitragekosten moet worden aangepast, en zij zullen onder andere het aantal arbitrages en de kosten en timing van de arbitrages in aanmerking nemen, waarbij er van wordt uitgegaan dat aan de deelnemende organisaties geen buitensporige financiële lasten zullen worden opgelegd. Het ministerie zal de Commissie in kennis stellen van het resultaat van deze evaluaties met de derde partij en zal de Commissie vooraf in kennis stellen van eventuele aanpassingen van het bedrag van de bijdragen. Honoraria voor advocaten vallen niet onder deze bepaling en worden ook niet gedekt door enig fonds uit hoofde van deze bepaling.

BIJLAGE II

UNITED STATES DEPARTMENT OF COMMERCE
Secretary of Commerce
Washington D.C. 20230

6 juli 2023

De heer Didier Reynders
Commissaris voor Justitie
Europese Commissie
Wetstraat 200
1049 Brussel
België

Geachte commissaris Reynders,

Namens de Verenigde Staten zend ik hierbij met genoegen een pakket met stukken over het EU-VS-kader voor gegevensbescherming dat, in combinatie met Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities" [Executive Order tot verbetering van de waarborgen voor activiteiten van de VS op het gebied van SIGINT] en 28 CFR deel 201 tot wijziging van de voorschriften van het ministerie van Justitie met het oog op de oprichting van de "Data Protection Review Court", belangrijke en gedetailleerde onderhandelingen weerspiegelt om de bescherming van de privacy en de burgerlijke vrijheden te versterken. Deze onderhandelingen hebben geleid tot nieuwe waarborgen die ervoor moeten zorgen dat de activiteiten van de VS op het gebied van SIGINT noodzakelijk en evenredig zijn bij het nastreven van bepaalde doelstellingen van nationale veiligheid en een nieuw verhaalsmechanisme voor natuurlijke personen in de Europese Unie ("EU") als zij menen dat zij onrechtmatig zijn geviseerd door activiteiten op het gebied van SIGINT, die samen de privacy van de persoonsgegevens van de EU zullen waarborgen. Het EU-VS-kader voor gegevensbescherming zal een inclusieve en concurrerende digitale economie ondersteunen. We mogen allebei trots zijn op de verbeteringen die in dat kader tot uiting komen en die de bescherming van de privacy in de hele wereld zullen verbeteren. Dit pakket biedt, samen met het Executive Order, regelgeving en andere documenten die via openbare bronnen beschikbaar zijn, een zeer sterke basis voor de vaststelling van een nieuw adequaatheidsbesluit door de Europese Commissie ([1]).

Het volgende materiaal is bijgevoegd:

— de beginselen van het EU-VS-kader voor gegevensbescherming, met inbegrip van de aanvullende beginselen (samen "de beginselen") en bijlage I bij de beginselen (d.w.z. een bijlage met de voorwaarden waaronder DPF-organisaties verplicht zijn te bemiddelen in bepaalde resterende vorderingen met betrekking tot onder de beginselen vallende persoonsgegevens);

— een brief van de dienst Internationale Handel van het ministerie, die het kaderprogramma voor gegevensbescherming beheert, met een beschrijving van de verbintenissen die ons ministerie is aangegaan om ervoor te zorgen dat het EU-VS-kader voor gegevensbescherming doeltreffend werkt;

— een brief van de Federal Trade Commission waarin haar handhaving van de beginselen wordt beschreven;

— een brief van het ministerie van Vervoer waarin zijn handhaving van de beginselen wordt beschreven;

— een door het Office of the Director of National Intelligence (bureau van de directeur van de nationale inlichtingendienst, hierna "ODNI") opgestelde brief met betrekking tot waarborgen en beperkingen die van toepassing zijn op de nationale veiligheidsdiensten van de VS; en

— een brief opgesteld door het Amerikaanse ministerie van Justitie met betrekking tot de waarborgen en beperkingen inzake de toegang van de Amerikaanse overheid ten behoeve van rechtshandhaving en het algemeen belang.

([1]) Op voorwaarde dat het besluit van de Commissie betreffende de gepastheid van de door het EU-VS-privacyschild geboden bescherming van toepassing is op IJsland, Liechtenstein en Noorwegen, zal het pakket van het EU-VS-kader voor gegevensbescherming op zowel de Europese Unie als deze drie landen van toepassing zijn.

Het volledige pakket van het EU-VS-kader voor gegevensbescherming zal worden bekendgemaakt op de DPF-website van het ministerie en de beginselen en bijlage I bij de beginselen zullen van kracht worden op de datum van inwerkingtreding van het adequaatheidsbesluit van de Europese Commissie.

U kunt ervan verzekerd zijn dat de Verenigde Staten deze toezeggingen ernstig nemen. Wij kijken ernaar uit met u samen te werken wanneer het EU-VS-kader voor gegevensbescherming is geïmplementeerd en we samen aan de volgende fase van dit proces beginnen.

Hoogachtend,

Gina M. RAIMONDO

BIJLAGE III

UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

12 december 2022

De heer Didier Reynders
Commissaris voor Justitie
Europese Commissie
Wetstraat 200
1049 Brussel
België

Geachte commissaris Reynders,

Namens de International Trade Administration ("ITA") beschrijf ik met genoegen de verbintenissen die het ministerie van Handel ("het ministerie") is aangegaan om de bescherming van persoonsgegevens te waarborgen via zijn beheer van en toezicht op het programma van het kader voor gegevensbescherming. De voltooiing van het EU-VS-kader voor gegevensbescherming ("EU-VS DPF") is een belangrijk resultaat voor de privacy en voor het bedrijfsleven aan beide zijden van de Atlantische Oceaan, aangezien het natuurlijke personen in de EU het vertrouwen zal schenken dat hun gegevens zullen worden beschermd en dat zij over rechtsmiddelen zullen beschikken om problemen in verband met hun gegevens aan te pakken, en duizenden bedrijven in staat zal stellen te blijven investeren en anderszins handel te blijven drijven over de Atlantische Oceaan heen, ten voordele van onze respectieve economieën en burgers. Het EU-VS-DPF is het resultaat van jarenlang hard werk en samenwerking met u en uw collega's in de Europese Commissie ("de Commissie"). Wij verheugen ons erop te blijven samenwerken met de Commissie om ervoor te zorgen dat deze gezamenlijke inspanning doeltreffend blijft werken.

Het EU-VS-DPF zal aanzienlijke voordelen opleveren voor zowel particulieren als bedrijven. Ten eerste biedt het een belangrijke reeks privacybeschermingen voor de gegevens van EU-burgers die aan de Verenigde Staten worden doorgegeven. Deelnemende organisaties in de VS moeten een conform privacybeleid ontwikkelen; zich er publiekelijk toe verbinden te voldoen aan de "beginselen van het EU-VS-kader voor gegevensbescherming", met inbegrip van de aanvullende beginselen (samen "de beginselen"), en bijlage I bij de beginselen (d.w.z. een bijlage met de voorwaarden waaronder EU-VS-DPF-organisaties verplicht zijn te bemiddelen in bepaalde resterende vorderingen met betrekking tot onder de beginselen vallende persoonsgegevens), zodat de verbintenis afdwingbaar wordt krachtens het recht van de Verenigde Staten ([1]); jaarlijks hun naleving bij het ministerie hercertificeren; kosteloze, onafhankelijke geschillenbeslechting bieden voor natuurlijke personen uit de EU; en onderworpen zijn aan de onderzoeks- en handhavingsautoriteit van een in de beginselen genoemde Amerikaanse wettelijke instantie (bv. de Federal Trade Commission (de "FTC") en het ministerie van Vervoer), of een Amerikaanse wettelijke instantie die in een toekomstige bijlage bij de beginselen wordt genoemd. De beslissing van een organisatie om zichzelf te certificeren is weliswaar vrijwillig, maar zodra een organisatie zich publiekelijk verbindt tot het EU-VS-DPF, kan haar verbintenis volgens de Amerikaanse wetgeving worden afgedwongen door de FTC, het ministerie van Vervoer of een andere Amerikaanse wettelijke instantie, afhankelijk van de vraag welke instantie jurisdictie heeft over de deelnemende organisatie. Ten tweede zal het EU-VS-DPF bedrijven in de Verenigde Staten,

([1]) Organisaties die zelf hun verbintenis tot naleving van de beginselen van het EU-VS-privacyschildkader hebben gecertificeerd en de voordelen van deelname aan het EU-VS-DPF willen genieten, moeten voldoen aan de "beginselen van het EU-VS-kader voor gegevensbescherming". Deze verbintenis tot naleving van de "beginselen van het EU-VS-kader voor gegevensbescherming" wordt zo spoedig mogelijk, en uiterlijk drie maanden na de datum van inwerkingtreding van de "beginselen van het EU-VS-kader voor gegevensbescherming", in het privacybeleid van die deelnemende organisaties opgenomen. (Zie hoofdstuk e) van het aanvullend beginsel inzake zelfcertificering).

met inbegrip van dochterondernemingen van Europese bedrijven in de Verenigde Staten, in staat stellen om persoonsgegevens te ontvangen vanuit de Europese Unie om gegevensstromen mogelijk te maken die de trans-Atlantische handel ondersteunen. De gegevensstromen tussen de Verenigde Staten en de Europese Unie zijn de grootste ter wereld en vormen de basis voor de economische relatie tussen de VS en de EU ter waarde van 7,1 biljoen USD, goed voor miljoenen banen aan beide zijden van de Atlantische Oceaan. Bedrijven die afhankelijk zijn van trans-Atlantische gegevensstromen komen uit alle industriële sectoren en omvatten grote Fortune 500-bedrijven evenals vele kleine en middelgrote ondernemingen. Trans-Atlantische gegevensstromen kunnen Amerikaanse organisaties in staat stellen gegevens te verwerken die nodig zijn om goederen, diensten en werkgelegenheid te bieden aan Europese burgers.

Het ministerie wil nauw en productief samenwerken met onze EU-collega's om het programma van het kader voor gegevensbescherming doeltreffend te beheren en te controleren. Dit streven komt tot uiting in de ontwikkeling en voortdurende verfijning door het ministerie van allerlei hulpmiddelen om organisaties te helpen bij het zelfcertificeringsproces, het opzetten van een website om belanghebbenden gerichte informatie te verstrekken, samenwerking met de Commissie en de Europese gegevensbeschermingsautoriteiten om richtsnoeren te ontwikkelen die belangrijke elementen van het EU-VS-DPF verduidelijken, voorlichting om een beter begrip van de gegevensbeschermingsverplichtingen van organisaties te bevorderen, en toezicht op en monitoring van de naleving van de programmavereisten door organisaties.

Dankzij onze voortdurende samenwerking met gewaardeerde EU-collega's zal het ministerie ervoor kunnen zorgen dat het EU-VS-DPF doeltreffend functioneert. De regering van de Verenigde Staten werkt al geruime tijd met de Commissie samen om gemeenschappelijke beginselen inzake gegevensbescherming te bevorderen, de verschillen in onze respectieve juridische aanpak te overbruggen en tegelijkertijd de handel en de economische groei in de Europese Unie en de Verenigde Staten te bevorderen. Wij geloven dat het EU-VS-DPF, dat een voorbeeld is van deze samenwerking, de Commissie in staat zal stellen een nieuw adequaatheidsbesluit te nemen dat organisaties in staat zal stellen het EU-VS-DPF te gebruiken om persoonsgegevens van de Europese Unie naar de Verenigde Staten door te geven in overeenstemming met de EU-wetgeving.

Beheer en toezicht inzake het programma van het kader voor gegevensbescherming door het ministerie van Handel

Het ministerie is vastbesloten het programma van het kader voor gegevensbescherming doeltreffend te beheren en te controleren en zal passende inspanningen leveren en passende middelen inzetten om dat resultaat te waarborgen. Het ministerie zal een gezaghebbende lijst bijhouden en voor het publiek toegankelijk maken van Amerikaanse organisaties die zichzelf bij het ministerie hebben gecertificeerd en zich ertoe hebben verbonden de beginselen na te leven ("de DPF-lijst"), die het zal bijwerken op basis van de jaarlijkse hercertificeringsaanvragen van de deelnemende organisaties en door organisaties te schrappen wanneer zij zich vrijwillig terugtrekken, de jaarlijkse hercertificering niet voltooien overeenkomstig de procedures van het ministerie, of permanent nalaten aan de regels te voldoen. Het ministerie houdt ook een gezaghebbend register bij van de Amerikaanse organisaties die uit de DPF-lijst zijn verwijderd en maakt dit voor het publiek toegankelijk, waarbij in elk afzonderlijk geval de reden voor die verwijdering wordt aangegeven. De bovengenoemde gezaghebbende lijst en het gezaghebbend register zullen voor het publiek beschikbaar blijven op de DPF-website van het ministerie. De DPF-website zal een duidelijk zichtbare verklaring bevatten dat elke organisatie die van de lijst van het kader voor gegevensbescherming wordt verwijderd, niet langer mag beweren dat zij deelneemt aan of voldoet aan het EU-VS-DPF en niet langer mag beweren dat zij persoonlijke informatie mag ontvangen op grond van het EU-VS-DPF. Een dergelijke organisatie moet niettemin de beginselen blijven toepassen op de persoonsgegevens die zij tijdens haar deelname aan het EU-VS-DPF heeft ontvangen, zolang zij deze informatie bewaart. Ter bevordering van zijn overkoepelende, voortdurende inzet voor een doeltreffend beheer van en toezicht op het kaderprogramma voor gegevensbescherming, verbindt het ministerie zich er met name toe het volgende te doen:

De inachtneming van de vereisten inzake zelfcertificering controleren

— Alvorens de eerste zelfcertificering of de jaarlijkse hercertificering van een organisatie (samen de "zelfcertificering") af te ronden en een organisatie op de DPF-lijst te plaatsen of te handhaven, gaat het ministerie na of de organisatie ten minste heeft voldaan aan de eisen van het aanvullend beginsel inzake zelfcertificering met betrekking tot de informatie die een organisatie in haar zelfcertificering aan het ministerie moet verstrekken, en te gepasten tijde een relevant privacybeleid heeft verstrekt dat personen informeert over alle 13 in het kennisgevingsbeginsel genoemde elementen. Het ministerie zal nagaan of de organisatie:

— de organisatie heeft aangeduid die haar zelfcertificering indient, alsmede alle Amerikaanse entiteiten of dochterondernemingen van de zelfcertificerende organisatie die ook de beginselen onderschrijven die de organisatie onder haar zelfcertificering wenst te laten vallen;

— de vereiste contactinformatie van de organisatie heeft verstrekt (bv. contactinformatie voor specifieke personen en/of kantoren binnen de zelfcertificerende organisatie die verantwoordelijk zijn voor de behandeling van klachten, verzoeken om toegang en andere kwesties die zich voordoen in het kader van het EU-VS-DPF);

— het doel of de doelen heeft beschreven waarvoor de organisatie de uit de Europese Unie ontvangen persoonlijke informatie zou verzamelen en gebruiken;

— heeft aangegeven welke persoonsgegevens uit de Europese Unie zouden worden ontvangen op grond van het EU-VS-DPF en derhalve onder haar zelfcertificering zouden vallen;

— indien de organisatie een openbare website heeft, het webadres heeft verstrekt waar het relevante privacybeleid direct beschikbaar is op die website, of indien de organisatie geen openbare website heeft, het ministerie een kopie heeft verstrekt van het relevante privacybeleid en van de plaats waar dat privacybeleid kan worden ingezien door de betrokken natuurlijke personen (d.w.z. de betrokken werknemers indien het relevante privacybeleid een personeelsbeleid is, of het publiek indien het relevante privacybeleid geen personeelsbeleid is);

— op het juiste ogenblik in haar relevante privacybeleid (d.w.z. aanvankelijk alleen in een ontwerp van privacybeleid dat samen met de aanvraag wordt ingediend indien het een eerste zelfcertificering betreft; anders in een definitief en eventueel gepubliceerd privacybeleid) een verklaring heeft opgenomen dat zij de beginselen naleeft en een hyperlink naar of het webadres van de DPF-website van het ministerie (bijvoorbeeld de homepage of de webpagina van de DPF-lijst);

— te gepasten tijde in haar relevante privacybeleid alle twaalf andere in het kennisgevingsbeginsel genoemde elementen heeft opgenomen (bijvoorbeeld de mogelijkheid voor de betrokken EU-persoon om onder bepaalde voorwaarden een beroep te doen op bindende arbitrage; de verplichting om persoonlijke informatie bekend te maken als reactie op een gerechtvaardigd verzoek van openbare instanties, onder meer ter voldoening aan de eisen in verband met veiligheid of rechtshandhaving; en haar aansprakelijkheid in geval van verdere doorgifte aan derde partijen);

— de officiële instantie heeft aanwezen die bevoegd is om tegen de organisatie ingediende vorderingen in verband met eventuele oneerlijke of misleidende praktijken en schendingen van wetten of regelgeving betreffende de privacybescherming te behandelen (en die is opgenomen in de beginselen of een toekomstige bijlage bij de beginselen);

— een privacyprogramma heeft aangewezen waarvan de organisatie lid is;

— heeft aangegeven of de relevante methode (d.w.z. de vervolgprocedures die zij moet verstrekken) om na te gaan of zij de beginselen naleeft, "zelfbeoordeling" (d.w.z. interne verificatie) of "externe toetsing van de naleving" (d.w.z. verificatie door een derde partij) is, en indien zij als relevante methode externe toetsing van de naleving heeft aangegeven, zij ook de derde partij heeft aangegeven die deze toetsing heeft voltooid;

— het passende onafhankelijke verhaalsmechanisme heeft aangeduid dat beschikbaar is om klachten in het kader van de beginselen te behandelen en de betrokkene kosteloos passende verhaalsmogelijkheden te bieden.

— Als de organisatie heeft gekozen voor een onafhankelijk verhaalsmechanisme van een particuliere geschillenbeslechtingsinstantie, heeft zij in haar desbetreffende privacybeleid een hyperlink naar of het webadres voor de website of het klachtenformulier van het mechanisme opgenomen dat beschikbaar is om onopgeloste klachten in het kader van de beginselen te onderzoeken.

— Als de organisatie verplicht is (d.w.z. met betrekking tot personeelsgegevens die in het kader van de arbeidsverhouding vanuit de Europese Unie worden doorgegeven) of ervoor heeft gekozen om met de bevoegde gegevensbeschermingsautoriteiten samen te werken bij het onderzoek en de oplossing van klachten in het kader van de beginselen, heeft zij verklaard dat zij zich ertoe verbindt om met de gegevensbeschermingsautoriteiten samen te werken en gevolg te geven aan hun bijbehorende adviezen om specifieke maatregelen te nemen om de beginselen na te leven.

— Het ministerie zal ook nagaan of de zelfcertificeringsverklaring van de organisatie in overeenstemming is met haar relevante privacybeleid. Wanneer een zelfcertificerende organisatie haar entiteiten of dochterondernemingen in de Verenigde Staten met een afzonderlijk, relevant privacybeleid wil afdekken, zal het ministerie ook het relevante privacybeleid van deze afgedekte entiteiten of dochterondernemingen onderzoeken om zich ervan te vergewissen dat zij alle in het kennisgevingsbeginsel vermelde vereiste elementen bevatten.

— Het ministerie zal samenwerken met wettelijke instanties (bijvoorbeeld FTC en het ministerie van Vervoer) om na te gaan of de organisaties onder de jurisdictie van de desbetreffende wettelijke instantie vallen die in hun zelfcertificeringsverklaringen is vermeld, wanneer het ministerie redenen heeft om eraan te twijfelen dat zij onder die jurisdictie vallen.

— Het ministerie zal samenwerken met instanties voor alternatieve geschillenbeslechting in de particuliere sector om na te gaan of de organisaties actief zijn geregistreerd voor het onafhankelijke verhaalsmechanisme dat zij in hun zelfcertificeringsverklaringen hebben vermeld; en werkt met die instanties samen om na te gaan of de organisaties actief zijn geregistreerd voor de externe nalevingscontrole die zij in hun zelfcertificeringsverklaringen hebben vermeld, wanneer die instanties beide soorten diensten aanbieden.

— Het ministerie zal samenwerken met de derde partij die door het ministerie is gekozen als bewaarder van de financiële middelen die via de vergoeding van het panel van gegevensbeschermingsautoriteiten (d.w.z. de jaarlijkse vergoeding ter dekking van de werkingskosten van het panel van gegevensbeschermingsautoriteiten) worden geïnd, om na te gaan of de organisaties die vergoeding voor het betrokken jaar hebben betaald, wanneer de organisaties de gegevensbeschermingsautoriteiten als het relevante onafhankelijke verhaalsmechanisme hebben aangewezen.

— Het ministerie zal samenwerken met de derde partij die door het ministerie is geselecteerd voor het beheer van arbitrages in het kader van het in bijlage I bij de beginselen genoemde arbitragefonds om na te gaan of de organisaties aan dat arbitragefonds hebben bijgedragen.

— Wanneer het ministerie tijdens zijn beoordeling van de door organisaties ingediende zelfcertificeringsverklaringen problemen vaststelt, zal het de organisaties ervan in kennis stellen dat zij al deze problemen moeten aanpakken binnen de door het ministerie aangewezen passende termijn ([2]). Het ministerie zal hen ook meedelen dat, indien zij niet binnen de door het ministerie vastgestelde termijnen reageren of hun zelfcertificering niet overeenkomstig de procedures van het ministerie voltooien, de ingediende zelfcertificering als geannuleerd zal worden beschouwd, en dat tegen elke onjuiste voorstelling van zaken over de deelname van een organisatie aan of de naleving van het EU-VS-DPF door de FTC, het ministerie van Vervoer of een andere relevante overheidsinstantie handhavingsmaatregelen kunnen worden genomen. Het ministerie zal de organisaties informeren via de contactmiddelen die de organisaties aan het ministerie hebben verstrekt.

Samenwerking faciliteren met instanties voor alternatieve geschillenbeslechting die diensten in verband met de beginselen verlenen

— Het ministerie zal samenwerken met instanties voor alternatieve geschillenbeslechting in de particuliere sector die onafhankelijke verhaalsmechanismen aanbieden en die onopgeloste klachten in het kader van de beginselen kunnen onderzoeken, om na te gaan of zij ten minste voldoen aan de vereisten van het aanvullende beginsel inzake geschillenbeslechting en handhaving. Het ministerie zal nagaan of deze instanties:

  — op hun openbare websites informatie opnemen over de beginselen en de diensten die zij in het kader van het EU-VS-DPF verlenen: 1) informatie over of een hyperlink naar de vereisten van de beginselen voor onafhankelijke verhaalsmechanismen; 2) een hyperlink naar de website van het kader voor gegevensbescherming van het ministerie; 3) een toelichting dat hun diensten inzake geschillenbeslechting in het kader van het EU-VS-DPF voor natuurlijke personen kosteloos zijn; 4) een beschrijving van de wijze waarop een klacht in verband met de beginselen kan worden ingediend; 5) de termijnen waarbinnen klachten inzake de beginselen worden behandeld; en 6) een beschrijving van het scala aan verhaalsmogelijkheden. Het ministerie zal de instanties tijdig in kennis stellen van belangrijke wijzigingen in het toezicht op en het beheer van het programma van het kader voor gegevensbescherming door het ministerie, wanneer dergelijke wijzigingen ophanden zijn of reeds zijn aangebracht en die wijzigingen relevant zijn voor de rol die de instanties in het kader van het EU-VS-DPF spelen;

([2]) Wat de hercertificering betreft, wordt bijvoorbeeld verwacht dat de organisaties al deze kwesties binnen de 45 dagen aanpakken, behoudens bepaling door het ministerie van een andere, passende termijn.

— jaarlijks een verslag publiceren met geaggregeerde statistieken over hun diensten inzake geschillenbeslechting, dat onder meer moet omvatten: 1) het totale aantal tijdens het verslagjaar ontvangen klachten in verband met de beginselen; 2) de soorten ontvangen klachten; 3) maatstaven inzake de kwaliteit van de geschillenbeslechting, zoals de tijd die met de verwerking van klachten gemoeid was; en 4) de resultaten van de ontvangen klachten, met name het aantal en de soorten genomen maatregelen of opgelegde sancties. Het ministerie zal de instanties specifieke, aanvullende richtsnoeren verstrekken over de informatie die zij in die jaarverslagen moeten verstrekken, waarbij die vereisten nader worden uitgewerkt (bv. een opsomming van de specifieke criteria waaraan een klacht moet voldoen om in het kader van het jaarverslag als een met de beginselen verband houdende klacht te worden beschouwd), alsook andere soorten informatie die zij moeten verstrekken (bv. als de instantie ook een met de beginselen verband houdende verificatiedienst verleent, een beschrijving van de wijze waarop de instantie feitelijke of potentiële belangenconflicten vermijdt in situaties waarin zij een organisatie zowel verificatiediensten als geschillenbeslechtingsdiensten verleent). In de aanvullende richtsnoeren van het ministerie zal ook worden aangegeven op welke datum de jaarverslagen van de instanties over de desbetreffende verslagperiode moeten worden gepubliceerd.

Follow-up van organisaties die willen worden of zijn verwijderd van de DPF-lijst

— Indien een organisatie zich wenst terug te trekken uit het EU-VS-DPF, zal het ministerie eisen dat de organisatie alle verwijzingen naar het EU-VS DPF waaruit zou kunnen worden opgemaakt dat zij blijft deelnemen aan het EU-VS DPF en dat zij persoonsgegevens kan ontvangen op grond van het EU-VS-DPF, uit haar privacybeleid verwijdert (zie de beschrijving van de verbintenis van het ministerie om te zoeken naar valse beweringen over deelname). Het ministerie zal ook eisen dat de organisatie een passende vragenlijst invult en aan het ministerie voorlegt om het volgende te verifiëren:

  — haar wens om zich terug te trekken;

  — wat zij zal doen met de persoonsgegevens die zij op grond van het EU-VS-DPF heeft ontvangen terwijl zij deelnam aan het EU-VS-DPF: a) deze gegevens bewaren, de beginselen op deze gegevens blijven toepassen en jaarlijks aan het ministerie bevestigen dat zij zich ertoe verbindt de beginselen op deze gegevens toe te passen; b) deze gegevens bewaren en deze gegevens op een andere toegestane wijze "passend" beschermen; of c) al deze gegevens tegen een bepaalde datum terugzenden of wissen; en

  — wie binnen de organisatie zal fungeren als permanent contactpunt voor vragen in verband met de beginselen.

— Indien een organisatie gekozen heeft voor a) zoals hierboven beschreven, zal het ministerie ook eisen dat de organisatie elk jaar na haar terugtrekking (d.w.z. op de eerste verjaardag van de terugtrekking, alsmede op elke volgende verjaardag, tenzij en totdat de organisatie op een andere toegestane wijze voor een "passende" bescherming van deze gegevens zorgt of al deze gegevens teruggeeft of wist en het ministerie hiervan in kennis stelt) een passende vragenlijst invult en indient om na te gaan wat zij met deze persoonsgegevens heeft gedaan, wat zij zal doen met de persoonsgegevens die zij nog bewaart, en wie binnen de organisatie als permanent contactpunt zal fungeren voor vragen in verband met de beginselen.

— Indien een organisatie haar zelfcertificering heeft laten verlopen (d.w.z. haar jaarlijkse hercertificering of haar naleving van de beginselen niet heeft voltooid, of om een andere reden, zoals terugtrekking, van de DPF-lijst is geschrapt), zal het ministerie haar opdragen een passende vragenlijst in te vullen en bij het ministerie in te dienen om na te gaan of zij zich wil terugtrekken of opnieuw wil certificeren:

  — en indien zij zich wenst terug te trekken, verder na te gaan wat zij zal doen met de persoonsgegevens die zij op grond van het EU-VS-DPF heeft ontvangen terwijl zij aan het EU-VS-DPF deelnam (zie eerdere beschrijving van wat een organisatie moet nagaan indien zij zich wenst terug te trekken);

  — en indien zij voornemens is zich opnieuw te certificeren, verder na te gaan dat zij tijdens het verstrijken van haar certificeringsstatus de beginselen heeft toegepast op persoonsgegevens die zij in het kader van het EU-VS-DPF heeft ontvangen, en te verduidelijken welke stappen zij zal nemen om de onopgeloste problemen aan te pakken die haar hercertificering hebben vertraagd.

— Als een organisatie om een van de volgende redenen van de DPF-lijst wordt verwijderd: a) terugtrekking uit het EU-VS-DPF, b) het niet voltooien van de jaarlijkse hercertificering van de naleving van de beginselen (d.w.z. de organisatie is wel met het jaarlijkse hercertificeringsproces begonnen, maar heeft het niet tijdig voltooid, of is er zelfs niet mee begonnen), of c) "permanente niet-naleving", stuurt het ministerie een kennisgeving aan de in de zelfcertificeringsverklaring van de organisatie genoemde contactpersoon/contactpersonen, waarin de reden voor de verwijdering wordt vermeld en wordt uitgelegd dat de organisatie niet langer expliciet of impliciet mag beweren dat zij deelneemt aan of voldoet aan het EU-VS-DPF en niet langer expliciet of impliciet mag beweren dat zij in het kader van het EU-VS-DPF persoonsgegevens mag ontvangen. In de kennisgeving, die ook andere inhoud kan bevatten die is afgestemd op de reden voor de verwijdering, zal worden aangegeven dat organisaties die een verkeerde voorstelling geven van hun deelname aan of naleving van het EU-VS-DPF, ook wanneer zij beweren dat zij aan het EU-VS-DPF deelnemen nadat zij van de DPF-lijst zijn verwijderd, het voorwerp kunnen uitmaken van handhavingsmaatregelen door de FTC, het ministerie van Vervoer of een andere relevante overheidsinstantie.

Valse beweringen van deelname opsporen en aanpakken

— Op een permanente basis, wanneer een organisatie: a) niet langer deelneemt aan het EU-VS-DPF, b) haar jaarlijkse hercertificering niet voltooit of de beginselen niet naleeft (d.w.z. ofwel met de jaarlijkse hercertificering is begonnen, maar deze niet tijdig heeft voltooid, ofwel zelfs niet is begonnen), c) geschrapt wordt als deelnemer aan het EU-VS-DPF, met name wegens "permanente niet-naleving", of d) de eerste zelfcertificering van haar naleving van de beginselen niet voltooit (d.w.z. met het eerste zelfcertificeringsproces is begonnen maar dit niet tijdig heeft voltooid), zal het ministerie ambtshalve nagaan of het relevante gepubliceerde privacybeleid van de organisatie geen verwijzingen naar het EU-VS-DPF bevat waaruit zou kunnen worden opgemaakt dat de organisatie deelneemt aan het EU-VS-DPF en dat zij persoonsgegevens mag ontvangen uit hoofde van het EU-VS-DPF. Indien het ministerie vaststelt dat dergelijke verwijzingen niet zijn verwijderd, zal het ministerie de organisatie ervan in kennis stellen dat, waar nodig, de zaak naar de bevoegde instantie zal worden verwezen voor eventuele handhavingsmaatregelen indien de organisatie een verkeerde voorstelling van haar deelname aan het EU-VS-DPF blijft geven. Het ministerie zal de organisatie informeren via de contactmiddelen die de organisatie aan het ministerie heeft verstrekt of zo nodig via andere passende middelen. Als de organisatie noch de verwijzingen verwijdert noch tot een verklaring van zelfcertificering inzake haar naleving in het kader van het EU-VS-DPF overgaat, zal het ministerie de zaak ambtshalve verwijzen naar de FTC, het ministerie van Vervoer, of een andere gepaste handhavingsinstantie of, in voorkomend geval, actie nemen om het keurmerk van het EU-VS-DPF te handhaven.

— Het ministerie zal andere inspanningen leveren om valse beweringen van deelname aan het EU-VS-DPF en oneigenlijk gebruik van het keurmerk van het EU-VS-DPF op te sporen, ook door organisaties die, in tegenstelling tot de hierboven beschreven organisaties, zelfs nooit met het zelfcertificeringsproces zijn begonnen (bijvoorbeeld door passende zoekopdrachten op internet om verwijzingen naar EU-VS-DPF in het privacybeleid van organisaties op te sporen). Wanneer het ministerie aan de hand van deze inspanningen valse beweringen over deelname aan het EU-VS-DPF en oneigenlijk gebruik van het keurmerk van het EU-VS-DPF vaststelt, zal het de organisatie ervan in kennis stellen dat het ministerie de zaak, zo nodig, voor mogelijke handhavingsmaatregelen zal doorverwijzen naar de bevoegde instantie indien de organisatie een verkeerde voorstelling van haar deelname aan het EU-VS-DPF blijft geven. Het ministerie zal de organisatie informeren via de eventuele contactmiddelen die de organisatie aan het ministerie heeft verstrekt of zo nodig via andere passende middelen. Als de organisatie noch de verwijzingen verwijdert noch tot een verklaring van zelfcertificering inzake haar naleving in het kader van het EU-VS-DPF overgaat, overeenkomstig de procedures van het ministerie, zal het ministerie de zaak ambtshalve verwijzen naar de FTC, het ministerie van Vervoer, of een andere gepaste handhavingsinstantie of, in voorkomend geval, actie nemen om het keurmerk van het EU-VS-DPF te handhaven.

— Het ministerie zal specifieke serieuze klachten over valse beweringen over deelname aan het EU-VS-DPF die het ontvangt (bv. klachten van de gegevensbeschermingsautoriteiten, onafhankelijke verhaalsmechanismen van instanties voor alternatieve geschillenbeslechting uit de particuliere sector, betrokkenen, bedrijven uit de EU en de VS en andere soorten derden) onmiddellijk onderzoeken en behandelen; en

— het ministerie kan andere passende corrigerende maatregelen nemen. In geval van onjuiste verklaringen tegenover het ministerie kan vervolging worden ingesteld op grond van de False Statements Act (18 U.S.C. § 1001).

Periodiek ambtshalve nalevingscontroles en evaluaties van het programma van het kader voor gegevensbescherming uitvoeren

— Het ministerie zal zich voortdurend inspannen om toezicht te houden op de daadwerkelijke naleving door de EU-VS-DPF-organisaties om problemen op te sporen waarvoor vervolgmaatregelen nodig zijn. Het ministerie zal met name ambtshalve routinecontroles ter plaatse uitvoeren bij willekeurig geselecteerde EU-VS-DPF-organisaties, alsook ad-hoccontroles ter plaatse bij specifieke EU-VS-DPF-organisaties wanneer potentiële tekortkomingen in de naleving worden vastgesteld (bv. potentiële tekortkomingen in de naleving die door derden onder de aandacht van het ministerie worden gebracht) om na te gaan: a) dat het contactpunt/de contactpunten die verantwoordelijk is/zijn voor de behandeling van klachten, verzoeken om toegang en andere kwesties die zich voordoen in het kader van het EU-VS-DPF, beschikbaar zijn; b) indien van toepassing, dat het privacybeleid van de organisatie gemakkelijk door het publiek kan worden geraadpleegd, zowel op de openbare website van de organisatie als via een hyperlink op de DPF-lijst; c) dat het privacybeleid van de organisatie blijft voldoen aan de in de beginselen beschreven eisen inzake zelfcertificering; en d) dat het door de organisatie aangewezen onafhankelijke verhaalsmechanisme beschikbaar is om klachten in het kader van het EU-VS-DPF te behandelen. Het ministerie zal ook actief het nieuws volgen voor berichten die geloofwaardig bewijs leveren van niet-naleving door EU-VS-DPF-organisaties.

— In het kader van het onderzoek naar de naleving zal het ministerie eisen dat een EU-VS DPF-organisatie een gedetailleerde vragenlijst invult en aan het ministerie voorlegt wanneer: a) het ministerie specifieke serieuze klachten heeft ontvangen over de naleving door een organisatie van de beginselen, b) een organisatie niet afdoende reageert op het verzoek van het ministerie om informatie over het EU-VS-DPF, of c) er geloofwaardige aanwijzingen zijn dat een organisatie niet voldoet aan haar verplichtingen in het kader van het EU-VS-DPF. Wanneer het ministerie een dergelijke gedetailleerde vragenlijst aan een organisatie heeft toegezonden en de organisatie niet op bevredigende wijze op de vragenlijst antwoordt, zal het ministerie de organisatie ervan in kennis stellen dat het ministerie, indien het geen tijdig en bevredigend antwoord van de organisatie ontvangt, de zaak voor mogelijke handhavingsmaatregelen zal doorverwijzen naar de bevoegde instantie. Het ministerie zal de organisatie informeren via de contactmiddelen die de organisatie aan het ministerie heeft verstrekt of zo nodig via andere passende middelen. Indien de organisatie niet tijdig een bevredigend antwoord geeft, zal het ministerie de zaak ambtshalve voorleggen aan de FTC, het ministerie van Vervoer of een andere bevoegde handhavingsinstantie, of andere passende maatregelen nemen om naleving te waarborgen. Het ministerie zal, waar nodig, in overleg treden met de bevoegde gegevensbeschermingsautoriteiten over dergelijke nalevingscontroles; en

— het ministerie zal het beheer van en het toezicht op het programma van het kader voor gegevensbescherming periodiek evalueren om ervoor te zorgen dat zijn toezichtsinspanningen, met inbegrip van eventuele inspanningen via het gebruik van zoekinstrumenten (bv. om na te gaan of er dode links zijn naar het privacybeleid van EU-VS-DPF-organisaties), geschikt zijn om bestaande en eventuele nieuwe problemen aan te pakken.

De DPF-website aanpassen aan specifieke doelgroepen

Het ministerie zal de DPF-website aanpassen aan de volgende doelgroepen: EU-burgers, EU-bedrijven, Amerikaanse bedrijven en gegevensbeschermingsautoriteiten. Het opnemen van materiaal dat rechtstreeks is gericht aan EU-burgers en EU-bedrijven zal de transparantie op een aantal manieren bevorderen. Voor EU-burgers wordt op de website duidelijk uitgelegd: 1) welke rechten het EU-VS-DPF aan EU-burgers biedt; 2) welke verhaalsmechanismen beschikbaar zijn voor EU-burgers wanneer ze van mening zijn dat een organisatie haar verplichting om aan de beginselen te voldoen, heeft geschonden; en 3) hoe ze informatie over de zelfcertificering van een organisatie met betrekking tot het EU-VS-DPF kunnen vinden. Voor EU-ondernemingen zal het gemakkelijker zijn om te controleren: 1) of een organisatie deelneemt aan het EU-VS-DPF; 2) op welke soort informatie de zelfcertificering inzake het EU-VS-DPF van een organisatie van toepassing is; 3) welk privacybeleid van toepassing is op de desbetreffende informatie; en 4) welke methode de organisatie gebruikt om haar naleving van de beginselen te controleren. Voor Amerikaanse bedrijven wordt duidelijk uitgelegd: 1) wat de voordelen zijn van deelname aan het EU-VS-DPF; 2) hoe men zich bij de EU-VS-DPF kan aansluiten, en hoe men zich opnieuw bij de EU-VS-DPF kan certificeren en zich eruit kan terugtrekken; en 3) hoe de Verenigde Staten het EU-VS-DPF beheren en handhaven. De opneming van materiaal dat rechtstreeks tot de gegevensbeschermingsautoriteiten is gericht (bijvoorbeeld informatie over het speciale contactpunt van het ministerie voor gegevensbeschermingsautoriteiten en een hyperlink naar inhoud in verband met de beginselen op de website van de FTC) zal zowel de samenwerking als de transparantie bevorderen. Het ministerie zal ook op ad-hocbasis samenwerken met de Commissie en het Europees Comité voor gegevensbescherming (“EDPB”) om aanvullend, actueel materiaal te ontwikkelen (bijvoorbeeld antwoorden op vaak gestelde vragen) voor gebruik op de DPF-website, wanneer die informatie het efficiënte beheer van en toezicht op het programma van het kader voor gegevensbescherming zou faciliteren.

De samenwerking met de gegevensbeschermingsautoriteiten faciliteren

Om de mogelijkheden voor samenwerking met de gegevensbeschermingsautoriteiten te verhogen, zal het ministerie voorzien in een speciale contactpersoon die functioneert als tussenpersoon voor de gegevensbeschermingsautoriteiten. In gevallen waarin een gegevensbeschermingsautoriteit, onder meer naar aanleiding van een klacht van een natuurlijke persoon uit de EU, van mening is dat een EU-VS-DPF-organisatie de beginselen niet naleeft, kan zij contact opnemen met de speciale contactpersoon bij het ministerie om de organisatie nader te laten beoordelen. Het ministerie zal zijn uiterste best doen om de afhandeling van de klacht bij de EU-VS-DPF-organisatie te faciliteren. Binnen 90 dagen na ontvangst van de klacht verstrekt het ministerie een update aan de gegevensbeschermingsautoriteit. De speciale contactpersoon zal ook verwijzingen ontvangen betreffende organisaties die ten onrechte beweren deel te nemen aan het EU-VS-DPF. De speciale contactpersoon houdt zich op de hoogte van alle zaken die de gegevensbeschermingsautoriteiten naar het ministerie hebben verwezen, en het ministerie verstrekt in de hieronder beschreven gezamenlijke evaluatie een verslag met een analyse van alle klachten die het in het betreffende jaar heeft ontvangen. De speciale contactpersoon zal de gegevensbeschermingsautoriteiten helpen informatie te zoeken over de zelfcertificering of eerdere deelname aan het EU-VS-DPF van een specifieke organisatie, en de contactpersoon zal vragen van de gegevensbeschermingsautoriteit beantwoorden over de naleving van specifieke EU-VS-DPF-vereisten. Het ministerie zal ook samenwerken met de Commissie en het EDPB inzake procedurele en administratieve aspecten van het panel van gegevensbeschermingsautoriteiten, met inbegrip van de vaststelling van passende procedures voor de verdeling van de via de vergoeding van het panel van gegevensbeschermingsautoriteiten geïnde middelen. Wij hebben begrepen dat de Commissie met het ministerie zal samenwerken om een oplossing voor eventuele problemen in verband met deze procedures te faciliteren. Bovendien zal het ministerie de gegevensbeschermingsautoriteiten voorzien van materiaal met betrekking tot het EU-VS-DPF, dat zij op hun eigen websites kunnen plaatsen om de transparantie voor natuurlijke personen en ondernemingen uit de EU te vergroten. Het toegenomen bewustzijn ten aanzien van het EU-VS-DPF en de rechten en plichten die het creëert moeten het gemakkelijker maken bepaalde kwesties in een vroeg stadium te constateren, zodat ze op de juiste wijze kunnen worden aangepakt.

De verbintenissen uit hoofde van bijlage I bij de beginselen nakomen

Het ministerie zal zijn verbintenissen uit hoofde van bijlage I bij de beginselen nakomen, met inbegrip van het bijhouden van een lijst van arbiters die het samen met de Commissie heeft gekozen op basis van onafhankelijkheid, integriteit en deskundigheid; en ondersteuning, waar nodig, van de derde partij die door het ministerie is geselecteerd om arbitrages te beheren overeenkomstig het in bijlage I bij de beginselen ([3])genoemde arbitragefonds. Het ministerie zal met de derde partij samenwerken om onder meer na te gaan of de derde partij een website bijhoudt met richtsnoeren over de arbitrageprocedure, waaronder: 1) hoe een procedure in te leiden en documenten in te dienen; 2) de lijst van arbiters die door het ministerie wordt bijgehouden en de wijze waarop arbiters uit die lijst kunnen worden gekozen; 3) de door het ministerie en de Commissie vastgestelde arbitrageprocedures en gedragscode voor arbiters ([4]); en 4) de inning en betaling van honoraria van arbiters. Bovendien zal het ministerie samenwerken met de derde partij om de werking van het arbitragefonds periodiek te evalueren, inclusief de vraag of het bedrag van de bijdragen of van de "caps" (de maximumbedragen) van de arbitragekosten moet worden aangepast, en zullen zij onder andere het aantal arbitrages en de kosten en timing van de arbitrages in aanmerking nemen, waarbij er van wordt uitgegaan dat aan de EU-VS-DPF-organisaties geen buitensporige financiële lasten zullen worden opgelegd. Het ministerie zal de Commissie in kennis stellen van het resultaat van deze evaluaties met de derde partij en zal de Commissie vooraf in kennis stellen van eventuele aanpassingen van het bedrag van de bijdragen.

Gezamenlijke evaluaties van de werking van het EU-VS-DPF

Het ministerie en andere instanties zullen, waar nodig, op gezette tijden vergaderingen beleggen met de Commissie, belanghebbende gegevensbeschermingsautoriteiten en passende vertegenwoordigers van het EDPB, waar het ministerie updates zal geven over het EU-VS-DPF. Tijdens de vergaderingen zullen actuele kwesties in verband met de werking, de uitvoering, het toezicht en de handhaving van het kaderprogramma voor gegevensbescherming worden besproken. In de vergaderingen kunnen, waar nodig, aanverwante onderwerpen worden besproken, zoals andere mechanismen voor gegevensdoorgifte waarvoor de waarborgen van het EU-VS-DPF gelden.

([3]) Het International Centre for Dispute Resolution ("ICDR"), de internationale afdeling van de American Arbitration Association ("AAA") (tezamen "ICDR-AAA"), is door het ministerie geselecteerd om de arbitrages te beheren overeenkomstig bijlage I bij de beginselen.

([4]) Op 15 september 2017 hebben het ministerie en de Commissie ingestemd met de vaststelling van een reeks arbitrageregels voor bindende arbitrageprocedures zoals beschreven in bijlage I bij de beginselen, alsmede een gedragscode voor arbiters die in overeenstemming is met algemeen aanvaarde ethische normen voor commerciële arbiters en bijlage I bij de beginselen. Het ministerie en de Commissie zijn overeengekomen de arbitrageregels en de gedragscode aan te passen aan de updates in het kader van het EU-VS-DPF, en het ministerie zal met het ICDR-AAA samenwerken om deze aanpassingen uit te voeren.

Actualisering van wetgeving

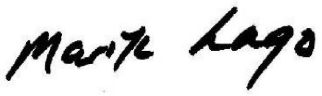
Het ministerie zal zich redelijke inspanningen getroosten om de Commissie te informeren over de materiële ontwikkelingen in de Amerikaanse wetgeving voor zover deze relevant zijn voor het EU-VS-DPF op het gebied van gegevensbescherming en de beperkingen en waarborgen die van toepassing zijn op de toegang van de Amerikaanse autoriteiten tot persoonsgegevens en het daaropvolgend gebruik van die gegevens.

Toegang van de Amerikaanse overheid tot persoonsgegevens

De Verenigde Staten hebben Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities" [Executive Order tot verbetering van de waarborgen voor activiteiten van de VS op het gebied van SIGINT] en 28 CFR deel 201 uitgevaardigd tot wijziging van de voorschriften van het ministerie van Justitie voor de oprichting van de Data Protection Review Court (de "DPRC"), die een sterke bescherming bieden voor persoonsgegevens met betrekking tot de toegang van de overheid tot gegevens voor doeleinden van nationale veiligheid. De geboden bescherming omvat: de versterking van de waarborgen inzake privacy en burgerlijke vrijheden om ervoor te zorgen dat de activiteiten van de VS op het gebied van SIGINT noodzakelijk en evenredig zijn voor het bereiken van vastgestelde doelstellingen in verband met de nationale veiligheid; de instelling van een nieuw verhaalsmechanisme met onafhankelijk en bindend gezag; en de verbetering van het bestaande strenge en gelaagde toezicht op de SIGINT-activiteiten van de Verenigde Staten. Door deze bescherming kunnen natuurlijke personen uit de EU verhaal halen bij een nieuw meerlagig verhaalsmechanisme dat een onafhankelijke DPRC omvat die zou bestaan uit personen van buiten de Amerikaanse overheid, die volledig bevoegd zouden zijn om vorderingen te beoordelen en zo nodig corrigerende maatregelen te nemen. Het ministerie zal een register bijhouden van natuurlijke personen in de EU die een in aanmerking komende klacht indienen uit hoofde van Executive Order 14086 en 28 CFR deel 201. Vijf jaar na de datum van deze brief, en vervolgens om de vijf jaar, zal het ministerie met de betrokken instanties contact opnemen over de vraag of informatie met betrekking tot de toetsing van in aanmerking komende klachten of de toetsing van bij de DPRC ingediende verzoeken om toetsing is gederubriceerd. Indien dergelijke informatie is gederubriceerd, zal het ministerie met de betrokken gegevensbeschermingsautoriteit samenwerken om de natuurlijke persoon in de EU te informeren. Deze verbeteringen bevestigen dat persoonsgegevens uit de EU die aan de Verenigde Staten worden doorgegeven, zullen worden behandeld op een wijze die strookt met de wettelijke voorschriften van de EU inzake toegang tot gegevens door de overheid.

Op grond van de beginselen, Executive Order 14086, 28 CFR deel 201 en de begeleidende brieven en documenten, waaronder de toezeggingen van het ministerie inzake het beheer van en het toezicht op het programma van het kader voor gegevensbescherming, verwachten wij dat de Commissie zal vaststellen dat het EU-VS-DPF adequate bescherming biedt met het oog op de EU-wetgeving en dat de doorgifte van gegevens uit de Europese Unie naar organisaties die deelnemen aan het EU-VS-DPF zal worden voortgezet. Wij verwachten ook dat doorgiften aan Amerikaanse organisaties op basis van modelcontractbepalingen of bindende bedrijfsvoorschriften van de EU door de voorwaarden van die regelingen verder zullen worden gefaciliteerd.

Hoogachtend,



Marisa LAGO

BIJLAGE IV

UNITED STATES OF AMERICA
Federal Trade Commission
Washington D.C. 20580

Office of the Chair

9 juni 2023

Didier Reynders
Commissaris voor Justitie
Europese Commissie
Wetstraat 200
1049 Brussel
België

Geachte commissaris Reynders,

De Federal Trade Commission van de Verenigde Staten ("FTC") stelt het op prijs dat zij de gelegenheid krijgt haar handhavingsrol in verband met de beginselen van het EU-VS-kader voor gegevensbescherming ("EU-VS-DPF") toe te lichten. De FTC zet zich al lang in voor de bescherming van consumenten en privacy over de grenzen heen en wij bevestigen onze verbintenis voor de handhaving van de commerciële aspecten van het EU-VS-DPF. De FTC vervult een dergelijke rol sinds 2000, in verband met het VS-EU-veiligehavenkader, en recentelijk sinds 2016, in verband met het EU-VS-privacyschildkader ([1]). Op 16 juli 2020 heeft het Hof van Justitie van de Europese Unie ("het Hof") het adequaatheidsbesluit van de Europese Commissie dat ten grondslag ligt aan het EU-VS-privacyschildkader nietig verklaard op grond van andere kwesties dan de commerciële beginselen die de FTC heeft gehandhaafd. De VS en de Europese Commissie hebben sindsdien onderhandeld over het EU-VS-kader voor gegevensbescherming om aan dat arrest van het Hof tegemoet te komen.

Ik richt dit schrijven tot u om te bevestigen dat de FTC zich inzet voor een krachtige handhaving van de EU-VS-DPF-beginselen. We bevestigen onze toezegging in het bijzonder op drie hoofdgebieden: 1) het geven van prioriteit aan verwijzingen en onderzoeken; 2) het aanvragen en opvolgen van bevelen; en 3) de samenwerking bij de handhaving met de gegevensbeschermingsautoriteiten van de EU.

I. **Inleiding**

a. **Handhaving door en beleidsactiviteiten van de FTC op het gebied van privacy**

De FTC heeft op het gebied van civiele handhaving een brede bevoegdheid voor de bevordering van consumentenbescherming en mededinging op het gebied van handel. Als onderdeel van haar mandaat op het gebied van gegevensbescherming handhaaft de FTC een breed scala aan wetten ter bescherming van de privacy en beveiliging van consumenten

([1]) Brief van voorzitter Edith Ramirez aan Věra Jourová, commissaris voor Justitie, Consumentenrechten en Gendergelijkheid van de Europese Commissie, met een beschrijving van de handhaving door de Federal Trade Commission van het nieuwe EU-VS-privacyschildkader (29 februari 2016), beschikbaar op https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. De FTC heeft zich er eerder ook toe verbonden het VS-EU-veiligehavenprogramma te handhaven. Brief van Robert Pitofsky, voorzitter van de FTC, aan John Mogg, directeur-generaal Interne markt, Europese Commissie (14 juli 2000), beschikbaar op https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission. Deze brief vervangt die eerdere toezeggingen.

en hun gegevens. De primaire wet die door de FTC wordt gehandhaafd, de FTC Act, verbiedt "oneerlijke" of "misleidende" handelingen of praktijken in het kader van of betrekking hebbend op handel ([2]). Ook handhaaft de FTC specifieke wetten die informatie over gezondheid, krediet en andere financiële aangelegenheden, alsook onlinegegevens van kinderen beschermen, en heeft zij regelgeving uitgevaardigd ter uitvoering van deze wetten ([3]).

De FTC heeft onlangs ook talrijke initiatieven genomen om haar werk op het gebied van privacy te versterken. In augustus 2022 kondigde de FTC aan dat zij regels overweegt om schadelijke commerciële surveillance en lakse gegevensbeveiliging aan te pakken ([4]). Het doel van het project is een solide openbaar verslag op te stellen om te informeren of de FTC regels moet uitvaardigen om commerciële surveillance- en gegevensbeveiligingspraktijken aan te pakken, en hoe die regels er mogelijk moeten uitzien. Opmerkingen van belanghebbenden in de EU over dit en andere initiatieven zijn welkom.

Op onze "PrivacyCon"-conferenties blijven vooraanstaande onderzoekers samenkomen om de nieuwste onderzoeken en trends op het gebied van privacy en gegevensbeveiliging te bespreken. We hebben ook het vermogen van onze instantie vergroot om gelijke tred te houden met de technologische ontwikkelingen die centraal staan in veel van ons privacywerk, door een groeiend team van technologen en interdisciplinaire onderzoekers op te bouwen. Zoals u weet, hebben wij ook een gezamenlijke dialoog met u en uw collega's bij de Europese Commissie aangekondigd, waarbij onder meer privacygerelateerde onderwerpen als donkere patronen en bedrijfsmodellen die worden gekenmerkt door alomtegenwoordige gegevensverzameling aan de orde komen ([5]). We hebben onlangs ook een rapport aan het Congres uitgebracht waarin we waarschuwen voor de schade die gepaard gaat met het gebruik van artificiële intelligentie ("AI") om door het Congres vastgestelde onlineschade aan te pakken. In dat rapport werd bezorgdheid geuit over onnauwkeurigheid, vooringenomenheid, discriminatie en commerciële surveillanceverschuiving ([6]).

b. **Juridische bescherming in de VS die ten goede komt aan EU-consumenten**

Het EU-VS-DPF zal worden uitgevoerd in de context van het bredere privacylandschap van de VS, waarin EU-consumenten op een aantal manieren worden beschermd. Het verbod op oneerlijke of misleidende handelingen of praktijken dat is opgenomen in de FTC Act is niet beperkt tot het beschermen van Amerikaanse consumenten tegen Amerikaanse bedrijven, aangezien het ook praktijken omvat die 1) redelijk voorzienbare schade veroorzaken of kunnen veroorzaken in de Verenigde Staten of 2) betrekking hebben op materiële gedragingen in de Verenigde Staten. Verder kan de FTC alle rechtsmiddelen die voor de bescherming van binnenlandse consumenten beschikbaar zijn, ook aanwenden ten behoeve van de bescherming van buitenlandse consumenten ([7]).

De FTC handhaaft tevens andere specifieke wetgeving die ook niet-Amerikaanse consumenten beschermt, zoals de Children's Online Privacy Protection Act (COPPA). De COPPA verplicht exploitanten van op kinderen gerichte websites en onlinediensten of websites voor het algemene publiek die doelbewust persoonsgegevens verzamelen van kinderen onder de 13 jaar, onder meer om de ouders in kennis te stellen en hun controleerbare toestemming te verkrijgen. Amerikaanse websites en diensten waarop de COPPA van toepassing is en door middel waarvan persoonsgegevens worden verzameld van buitenlandse kinderen, moeten de COPPA in acht nemen. Buitenlandse websites en onlinediensten moeten ook aan de

([2]) 15 U.S.C. § 45, (a). De FTC is niet bevoegd voor strafrechtelijke handhaving of kwesties in verband met de nationale veiligheid. Evenmin heeft de FTC invloed op de meeste andere acties van overheidswege. Bovendien bestaan er uitzonderingen op de rechtsbevoegdheid van de FTC ten aanzien van commerciële activiteiten, onder meer met betrekking tot banken, luchtvaartmaatschappijen, het verzekeringswezen en de algemene transmissieactiviteiten van dienstverleners in de telecommunicatie. Ook heeft de FTC geen rechtsbevoegdheid over de meeste non-profitorganisaties, maar wel over frauduleuze liefdadige instellingen of andere non-profitorganisaties die in feite met een winstoogmerk handelen. De FTC heeft ook rechtsbevoegdheid over non-profitorganisaties die commerciële activiteiten ontplooien ten behoeve van hun leden die winst beogen, bijvoorbeeld door die leden aanzienlijke economische voordelen te bieden. In sommige gevallen valt de rechtsbevoegdheid van de FTC samen met die van andere rechtshandhavingsinstanties. We hebben een goede werkrelatie opgebouwd met federale en deelstaatsinstanties en werken nauw met deze instanties samen om onderzoeken te coördineren of zo nodig zaken ernaar te verwijzen.

([3]) *Zie* FTC, Privacy and Security" [privacy en veiligheid], https://www.ftc.gov/business-guidance/privacy-security.

([4]) Zie persbericht, Federal Trade Commission, "FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices" [FTC onderzoekt regels om commerciële surveillance en lakse gegevensbeveiligingspraktijken aan te pakken] (11 augustus 2022),https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices

([5]) Zie de gezamenlijke persverklaring van Didier Reynders, commissaris voor Justitie van de Europese Commissie, en Lina Khan, voorzitter van de Federal Trade Commission van de Verenigde Staten (30 maart 2022), beschikbaar op https://www.ftc.gov/system/files/ftc_gov/pdf/Joint FTC-EC Statement informal dialogue consumer protection issues.pdf.

([6]) Zie persbericht, Federal Trade Commission, FTC Report Warns About Using Artificial Intelligence to Combat Online Problems [FTC-rapport waarschuwt voor gebruik van artificiële intelligentie om online problemen aan te pakken] (16 juni 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.

([7]) 15 U.S.C. § 45, (a), (4), (B). Voorts omvatten "oneerlijke of misleidende handelingen of praktijken" handelingen of praktijken in de buitenlandse handel die i) binnen de Verenigde Staten redelijkerwijs voorzienbare schade veroorzaken of kunnen veroorzaken; of ii) materieel gedrag betreffen dat binnen de Verenigde Staten plaatsvindt. 15 U.S.C. § 45, (a), (4), (A).

COPPA-bepalingen voldoen als zij gericht zijn op kinderen in de Verenigde Staten of als daarmee doelbewust persoonsgegevens worden verzameld van kinderen in de Verenigde Staten. Naast de federale Amerikaanse wetten die door de FTC worden gehandhaafd kan andere federale en deelstaatswetgeving inzake consumentenbescherming, datalekken en privacy EU-consumenten bovendien nog meer voordelen bieden.

c. **Handhavingsactiviteiten van de FTC**

De FTC heeft zaken aanhangig gemaakt uit hoofde van zowel het VS-EU-veiligehavenkader als het EU-VS-privacyschildkader en is het EU-VS-privacyschild blijven handhaven, zelfs na de nietigverklaring door het Hof van het adequaatheidsbesluit dat ten grondslag ligt aan het EU-VS-privacyschildkader ([8]). In verschillende recente klachten van de FTC wordt aangevoerd dat bedrijven de bepalingen van het EU-VS-privacyschild hebben geschonden, onder meer in procedures tegen Twitter ([9]), CafePress ([10]) en Flo ([11]). In de handhavingsactie tegen Twitter heeft de FTC 150 miljoen USD van Twitter verkregen wegens schending van een eerder bevel van de FTC met praktijken die meer dan 140 miljoen klanten treffen, waaronder schending van beginsel 5 van het EU-VS-privacyschild (gegevensintegriteit en doelbinding). Voorts vereist het bevel van de FTC dat Twitter gebruikers in staat stelt veilige multifactorauthenticatiemethoden te gebruiken waarvoor gebruikers hun telefoonnummer niet hoeven te verstrekken.

In de zaak CafePress voerde de FTC aan dat het bedrijf de gevoelige informatie van consumenten niet had beveiligd, een grote gegevensinbreuk had verdoezeld en de beginselen 2 (keuze), 4 (beveiliging) en 6 (toegang) van het EU-VS-privacyschild had geschonden. Volgens het bevel van de FTC moet het bedrijf inadequate authenticatiemaatregelen vervangen door multifactorauthenticatie, de hoeveelheid gegevens die het verzamelt en bewaart aanzienlijk beperken, socialezekerheidsnummers versleutelen en een derde partij zijn informatiebeveiligingsprogramma's laten beoordelen en de FTC een kopie daarvan verstrekken die openbaar mag worden gemaakt.

In de zaak Flo voerde de FTC aan dat de vruchtbaarheidstraceerapp gezondheidsinformatie van gebruikers bekendmaakte aan derde aanbieders van gegevensanalyses nadat het bedrijf had toegezegd die informatie privé te houden. In de klacht van de FTC wordt specifiek gewezen op de interacties van het bedrijf met EU-consumenten en op het feit dat Flo de beginselen 1 (kennisgeving), 2 (keuze), 3 (verantwoordingsplicht voor verdere doorgifte) en 5 (gegevensintegriteit en doelbinding) van het EU-VS-privacyschild heeft geschonden. Het bevel van de FTC vereist onder meer dat Flo de betrokken gebruikers in kennis stelt van de openbaarmaking van hun persoonsgegevens en derden die gezondheidsinformatie van gebruikers hebben ontvangen, opdraagt deze gegevens te vernietigen. We benadrukken dat FTC-besluiten wereldwijd alle consumenten die zaken doen met een Amerikaans bedrijf beschermen, en niet slechts de consumenten die een klacht hebben ingediend.

In veel vroegere handhavingszaken met betrekking tot het VS-EU-veiligehavenkader en het EU-VS-privacyschild ging het om organisaties die een eerste zelfcertificering via het ministerie van Handel voltooiden, maar verzuimden hun jaarlijkse zelfcertificering te handhaven terwijl zij zich bleven voordoen als actuele deelnemers. In andere gevallen ging het om valse beweringen van deelname door organisaties die nooit een eerste zelfcertificering via het ministerie van Handel hadden voltooid. In de toekomst verwachten wij onze handhavingsinspanningen proactief te concentreren op het soort inhoudelijke schendingen van de EU-VS-DPF-beginselen die in zaken zoals Twitter, CafePress en Flo worden aangevoerd. Ondertussen zal het ministerie van Handel het zelfcertificeringsproces beheren en er toezicht op houden, de gezaghebbende lijst van deelnemers aan het EU-VS-DPF bijhouden en andere kwesties in verband met deelname aan het programma behandelen ([12]). Belangrijk is dat organisaties die aanspraak maken op deelname aan het EU-VS-DPF onderworpen kunnen worden aan inhoudelijke handhaving van de EU-VS-DPF-beginselen, zelfs indien zij hun zelfcertificering niet via het ministerie van Handel doen of handhaven.

([8]) Zie aanhangsel A voor een lijst van FTC-zaken op het gebied van de veilige haven en het privacyschild.

([9]) Zie persbericht, Federal Trade Commission, "FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads" [FTC beschuldigt Twitter van misleidend gebruik van accountbeveiligingsgegevens om gerichte advertenties te verkopen] (25 mei 2022), beschikbaar op https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

([10]) Zie persbericht, Federal Trade Commission, "FTC Takes Action Against CafePress for Data Breach Cover Up" [FTC onderneemt actie tegen CafePress wegens het toedekken van een datalek] (15 maart 2022), beschikbaar op https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

([11]) Zie persbericht, Federal Trade Commission, "FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others" [FTC rondt bevel af tegen Flo Health, een vruchtbaarheidstraceerapp die gevoelige gezondheidsgegevens deelde met Facebook, Google en anderen] (22 juni 2021), beschikbaar op, https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

([12]) Brief van Marisa Lago, onderminister van Handel voor Internationale Handel, aan Didier Reynders, Commissaris voor Justitie, Europese Commissie (12 december 2022).

II. **Het verlenen van prioriteit aan verwijzingen en onderzoeken**

Net als bij het VS-EU-veiligehavenkader en het EU-VS-privacyschildkader verbindt de FTC zich ertoe voorrang te geven aan verwijzingen van het ministerie van Handel en de EU-lidstaten in verband met de EU-VS DPF-beginselen. Wij zullen ook prioriteit geven aan de behandeling van verwijzingen wegens niet-naleving van de EU-VS-DPF-beginselen door zelfregulerende organisaties op het gebied van de privacy en andere onafhankelijke geschillenbeslechtingsinstanties.

Om verwijzingen van EU-lidstaten op grond van het EU-VS-DPF te vereenvoudigen, heeft de FTC een gestandaardiseerd verwijzingsproces opgezet en richtsnoeren voor EU-lidstaten opgesteld over de informatie die de FTC het best kan gebruiken bij haar onderzoek inzake een verwijzing. Een onderdeel hiervan is dat de FTC een contactpunt heeft aangewezen voor verwijzingen uit EU-lidstaten. Het is bijzonder nuttig wanneer de verwijzende instantie een voorlopig onderzoek heeft uitgevoerd naar de vermeende schending en met de FTC kan samenwerken tijdens het onderzoek.

Na ontvangst van een dergelijke verwijzing van het ministerie van Handel, een EU-lidstaat, een zelfregulerende organisatie of andere onafhankelijke geschillenbeslechtingsinstanties kan de FTC een aantal acties ondernemen om de aangekaarte problemen aan te pakken. Wij kunnen bijvoorbeeld het privacybeleid van de organisatie onderzoeken, rechtstreeks bij de organisatie of bij derden nadere informatie opvragen, de verwijzende instantie nader raadplegen, beoordelen of er een patroon van schendingen bestaat of sprake is van een aanzienlijk aantal getroffen consumenten, vaststellen of de verwijzing implicaties heeft die binnen de bevoegdheid van het ministerie van Handel vallen, beoordelen of extra inspanningen om de marktdeelnemers in gebreke te stellen, nuttig zouden zijn en, in voorkomend geval, een handhavingsprocedure starten.

Naast het geven van prioriteit aan verwijzingen uit hoofde van de EU-VS-DPF-beginselen door het ministerie van Handel, EU-lidstaten en zelfregulerende organisaties op het gebied van privacy of andere onafhankelijke geschillenbeslechtingsinstanties ([13]), zal de FTC waar nodig op eigen initiatief belangrijke schendingen van de EU-VS-DPF-beginselen blijven onderzoeken met behulp van een reeks instrumenten. Als onderdeel van het onderzoeksprogramma van de FTC naar privacy- en veiligheidskwesties waarbij commerciële organisaties betrokken zijn, heeft de dienst routinematig onderzocht of de betrokken entiteit beweringen deed over het EU-VS-privacyschild. Als de entiteit dergelijke beweringen deed en uit het onderzoek bleek dat de beginselen van het EU-VS-privacyschild kennelijk waren geschonden, dan nam de FTC de beschuldigingen van schending van de beginselen van het EU-VS-privacyschild in aanmerking bij haar handhavingsmaatregelen. Wij zullen deze proactieve aanpak voortzetten, nu met betrekking tot de EU-VS-DPF-beginselen.

III. **Verzoek om en toezicht op bevelen**

De FTC bevestigt tevens haar toezeggingen om toezicht te houden op de uitvoering van handhavingsbesluiten teneinde de naleving van de EU-VS-DPF-beginselen te verzekeren. Wij zullen tot naleving van EU-VS-DPF-beginselen verplichten door in de toekomst in bevelen van de FTC dwingende bepalingen inzake de EU-VS-DPF-beginselen op te nemen. Schendingen van de administratieve bevelen van de FTC kunnen leiden tot civiele boeten tot maximaal 50 120 USD per schending of 50 120 USD per dag in geval van voortgaande schending ([14]), die in geval van praktijken waar veel consumenten bij betrokken zijn, kunnen oplopen tot miljoenen dollars. In elke *consent order* zijn tevens rapportage- en nalevingsbepalingen opgenomen. De entiteiten waarop deze uitspraak van kracht is, moeten gedurende een specifiek aantal jaren documenten bijhouden waaruit hun naleving blijkt. De uitspraken moeten ook worden verspreid onder de werknemers die ervoor moeten zorgen dat de uitspraak ten uitvoer wordt gelegd.

De FTC houdt systematisch toezicht op de naleving van de bestaande bevelen op het gebied van de EU-VS-privacyschildbeginselen, zoals zij dat met al haar bevelen doet, en stelt zo nodig rechtsvorderingen in om de naleving ervan af te dwingen ([15]). We benadrukken dat FTC-besluiten wereldwijd alle consumenten die zaken doen met een bedrijf blijven beschermen, en niet slechts de consumenten die een klacht hebben ingediend. Ten slotte zal de FTC online een lijst bijhouden van de bedrijven waartegen bevelen zijn uitgevaardigd in verband met de handhaving van de EU-VS-DPF-beginselen ([16]).

([13]) Hoewel de FTC geen individuele klachten van consumenten oplost of hierin bemiddelt, bevestigt de FTC dat zij van Europese gegevensbeschermingsinstanties afkomstige verwijzingen in het kader van de EU-VS-DPF-beginselen prioriteit geeft. Daarnaast gebruikt de FTC klachten in haar Consumer Sentinel-databank, die voor veel andere wetshandhavingsinstanties toegankelijk is, om de richting van ontwikkelingen te bepalen, handhavingsprioriteiten vast te stellen en mogelijke onderzoeksdoelen vast te stellen. Natuurlijke personen uit de EU kunnen gebruikmaken van hetzelfde klachtensysteem dat beschikbaar is voor Amerikaanse consumenten om een klacht in te dienen bij de FTC op: https://reportfraud.ftc.gov/. Voor individuele klachten in het kader van de EU-VS-DPF-beginselen kan het voor natuurlijke personen in de EU echter zeer nuttig zijn om klachten in te dienen bij de gegevensbeschermingsinstantie in hun lidstaat of bij een onafhankelijke geschillenbeslechtingsinstantie.

([14]) 15 U.S.C. § 45, (m); 16 C.F.R. § 1.98. Dit bedrag wordt periodiek aangepast aan de inflatie.

([15]) Vorig jaar besloot de FTC om de procedure voor het onderzoeken van recidivisten te stroomlijnen. Zie persbericht, Federal Trade Commission, "FTC Authorizes Investigations into Key Enforcement Priorities" [De FTC geeft toestemming voor onderzoeken naar belangrijke handhavingsprioriteiten] (1 juli 2021), beschikbaar op https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.

([16]) Zie FTC, Privacy Shield, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. **Samenwerking op het gebied van handhaving met de Europese gegevensbeschermingsautoriteiten**

De FTC erkent de belangrijke rol die Europese gegevensbeschermingsautoriteiten spelen met betrekking tot de naleving van de EU-VS-DPF-beginselen en moedigt meer raadpleging en samenwerking op het gebied van handhaving aan. Een gecoördineerde aanpak van de uitdagingen die de huidige ontwikkelingen op de digitale markten en gegevensintensieve bedrijfsmodellen met zich meebrengen, wordt steeds belangrijker. De FTC zal informatie over verwijzingen uitwisselen met verwijzende handhavingsinstanties, onder meer over de stand van zaken met betrekking tot de verwijzing, met inachtneming van de wetgeving en de beperkingen op het gebied van vertrouwelijkheid. Voor zover mogelijk gelet op het aantal en het soort ontvangen verwijzingen, omvat de te verstrekken informatie een beoordeling van de verwezen zaken, waaronder een beschrijving van belangrijke kwesties die worden aangekaart en eventuele maatregelen die in het kader van de bevoegdheid van de FTC zijn genomen om schending van de wet aan te pakken. De FTC verstrekt ook feedback aan de verwijzende instantie over de soorten verwijzingen die zijn ontvangen om zo de doeltreffendheid van inspanningen om onrechtmatige gedrag aan te pakken, te verhogen. Wanneer een verwijzende handhavingsinstantie met het oog op het instellen van haar eigen handhavingsprocedure informatie wil over de stand van zaken met betrekking tot een specifieke verwijzing, zal de FTC, rekening houdend met het aantal in behandeling zijnde verwijzingen en onder voorbehoud van vertrouwelijkheid en andere wettelijke vereisten, reageren.

De FTC zal ook nauw samenwerken met de gegevensbeschermingsautoriteiten in de EU voor het verlenen van bijstand bij de handhaving. In passende gevallen kan het daarbij ook gaan om het delen van informatie en het verlenen van bijstand bij onderzoek op grond van de U.S. Safe Web Act, die de FTC de bevoegdheid verleent om buitenlandse rechtshandhavingsinstanties bij te staan wanneer deze wetgeving handhaven die praktijken verbiedt die in materiële zin vergelijkbaar zijn met die welke worden verboden door wetten die de FTC handhaaft ([17]). Als onderdeel van deze bijstand kan de FTC informatie delen die is verkregen in verband met een FTC-onderzoek, een getuigenoproeping gelasten namens de Europese gegevensbeschermingsautoriteiten die hun eigen onderzoek uitvoeren, en een mondelinge getuigenis afnemen van getuigen of gedaagden in verband met de handhavingsprocedure van de gegevensbeschermingsautoriteit, met inachtneming van de vereisten in de U.S. Safe Web Act. De FTC maakt regelmatig gebruik van deze bevoegdheid om andere instanties waar ook ter wereld bij te staan in zaken aangaande privacy en consumentenbescherming.

Naast eventueel overleg met verwijzende gegevensbeschermingsautoriteiten in de EU over specifieke zaken, zal de FTC deelnemen aan periodieke vergaderingen met aangewezen vertegenwoordigers van het Europees Comité voor gegevensbescherming ("EDPB") om in het algemeen te bespreken hoe de samenwerking op het gebied van handhaving kan worden verbeterd. De FTC zal, samen met het ministerie van Handel, de Europese Commissie en vertegenwoordigers van het EDPB, ook deelnemen aan de periodieke beoordeling van het EU-VS-DPF, waarbij de uitvoering ervan zal worden besproken. De FTC stimuleert tevens de ontwikkeling van instrumenten die de samenwerking op het gebied van handhaving bevorderen met Europese gegevensbeschermingsautoriteiten en andere handhavingsautoriteiten op het gebied van privacy wereldwijd. De FTC bevestigt met genoegen haar verbintenis voor de handhaving van de commerciële aspecten van het EU-VS-DPF. Wij zien ons partnerschap met EU-collega's als een cruciaal onderdeel van de bescherming van de privacy van onze en uw burgers.

Hoogachtend,

Lina M. KHAN
Chair, Federal Trade Commission

([17]) Bij de bepaling of zij haar bevoegdheid op grond van de U.S. Safe WEB Act zal uitoefenen, neemt de FTC onder andere het volgende in overweging: (A) of de verzoekende instantie heeft ingestemd met het verstrekken van wederzijdse bijstand aan de FTC of deze bijstand zal verstrekken; B) of het voldoen aan het verzoek het openbaar belang van de Verenigde Staten in het gedrang zal brengen; en (C) of de onderzoeks- of handhavingsprocedure van de verzoekende instantie betrekking heeft op handelingen of praktijken die aan een aanzienlijk aantal personen schade toebrengen of waarschijnlijk kunnen toebrengen. 15 U.S.C. § 46, (j), (3). Deze bevoegdheid is niet van toepassing op de handhaving van mededingingswetgeving.

Aanhangsel A

Handhaving van het privacyschild en de veilige haven

	Rolnummer/FTC-dossiernummer	Zaak	Link
1	FTC-dossiernummer 2023062 Zaak nr. 3:22-cv-03070 (N.D. Cal.)	US/**Twitter, Inc.**	Twitter
2	FTC-dossiernummer 192 3209	In de zaak Residual Pumpkin Entity, LLC, voorheen handelend onder de naam **CafePress**, en PlanetArt, LLC, voorheen handelend onder de naam **CafePress**	CafePress
3	FTC-dossiernummer 192 3133 Rolnummer C-4747	In de zaak **Flo Health, Inc.**	Flo Health
4	FTC-dossiernummer 192 3050 Rolnummer C-4723	In de zaak **Ortho-Clinical Diagnostics, Inc.**	Ortho-Clinical
5	FTC-dossiernummer 192 3092 Rolnummer C-4709	In de zaak **T&M Protection, LLC**	T&M Protection
6	FTC-dossiernummer 192 3084 Rolnummer C-4704	In de zaak **TDARX, Inc.**	TDARX
7	FTC-dossiernummer 192 3093 Rolnummer C-4706	In de zaak **Global Data Vault, LLC**	Global Data
8	FTC-dossiernummer 192 3078 Rolnummer C-4703	In de zaak **Incentive Services, Inc.**	Incentive Services
9	FTC-dossiernummer 192 3090 Rolnummer C-4705	In de zaak **Click Labs, Inc.**	Click Labs
10	FTC-dossiernummer 182 3192 Rolnummer C-4697	In de zaak **Medable, Inc.**	Medable
11	FTC-dossiernummer 182 3189 Rolnummer 9386	In de zaak NTT Global Data Centers Americas, Inc., als rechtsopvolger van **RagingWire Data Centers, Inc.**	RagingWire
12	FTC-dossiernummer 182 3196 Rolnummer C-4702	In de zaak **Thru, Inc.**	Thru
13	FTC-dossiernummer 182 3188 Rolnummer C-4698	In de zaak **DCR Workforce, Inc.**	DCR Workforce
14	FTC-dossiernummer 182 3194 Rolnummer C-4700	In de zaak **LotaData, Inc.**	LotaData
15	FTC-dossiernummer 182 3195 Rolnummer C-4701	In de zaak **EmpiriStat, Inc.**	EmpiriStat

16	FTC-dossiernummer 182 3193 Rolnummer C-4699	In de zaak 214 Technologies, Inc., ook voorheen handelend onder de naam **Trueface.ai**	Trueface.ai
17	FTC-dossiernummer 182 3107 Rolnummer 9383	In de zaak **Cambridge Analytica, LLC**	Cambridge Analytica
18	FTC-dossiernummer 182 3152 Rolnummer C-4685	In de zaak **SecureTest, Inc.**	SecurTest
19	FTC-dossiernummer 182 3144 Rolnummer C-4664	In de zaak **VenPath, Inc.**	VenPath
20	FTC-dossiernummer 182 3154 Rolnummer C-4666	In de zaak **SmartStart Employment Screening, Inc.**	SmartStart
21	FTC-dossiernummer 182 3143 Rolnummer C-4663	In de zaak **mResourceLLC,** voorheen handelend onder de naam Loop Works LLC	mResource
22	FTC-dossiernummer 182 3150 Rolnummer C-4665	In de zaak **Idmission LLC**	IDmission
23	FTC-dossiernummer 182 3100 Rolnummer C-4659	In de zaak **ReadyTech Corporation**	ReadyTech
24	FTC-dossiernummer 172 3173 Rolnummer C-4630	In de zaak **Decusoft, LLC**	Decusoft
25	FTC-dossiernummer 172 3171 Rolnummer C-4628	In de zaak **Tru Communication, Inc.**	Tru
26	FTC-dossiernummer 172 3172 Rolnummer C-4629	In de zaak **Md7, LLC**	Md7
30	FTC-dossiernummer 152 3198 Rolnummer C-4543	In de zaak **Jhayrmaine Daniels (voorheen handelend onder de naam California Skate-Line)**	Jhayrmaine Daniels
31	FTC-dossiernummer 152 3190 Rolnummer C-4545	In de zaak **Dale Jarrett Racing Adventure, Inc.**	Dale Jarrett
32	FTC-dossiernummer 152 3141 Rolnummer C-4540	In de zaak **Golf Connect, LLC**	Golf Connect
33	FTC-dossiernummer 152 3202 Rolnummer C-4546	In de zaak **Inbox Group, LLC**	Inbox Group
34	FTC-dossiernummer 152 3187 Rolnummer C-4542	In de zaak **IOActive, Inc.**	IOActive
35	FTC-dossiernummer 152 3140 Rolnummer C-4549	In de zaak **Jubilant Clinsys, Inc.**	Jubilant
36	FTC-dossiernummer 152 3199 Rolnummer C-4547	In de zaak **Just Bagels Manufacturing, Inc.**	Just Bagels

37	FTC-dossiernummer 152 3138 Rolnummer C-4548	In de zaak **NAICS Association, LLC**	NAICS
38	FTC-dossiernummer 152 3201 Rolnummer C-4544	In de zaak **One Industries Corp.**	One Industries
39	FTC-dossiernummer 152 3137 Rolnummer C-4550	In de zaak **Pinger, Inc.**	Pinger
40	FTC-dossiernummer 152 3193 Rolnummer C-4552	In de zaak **SteriMed Medical Waste Solutions**	SteriMed
41	FTC-dossiernummer 152 3184 Rolnummer C-4541	In de zaak **Contract Logix, LLC**	Contract Logix
42	FTC-dossiernummer 152 3185 Rolnummer C-4551	In de zaak **Forensics Consulting Solutions, LLC**	Forensics Consulting
43	FTC-dossiernummer 152 3051 Rolnummer C-4526	In de zaak **American Int'l Mailing, Inc.**	AIM
44	FTC-dossiernummer 152 3015 Rolnummer C-4525	In de zaak **TES Franchising, LLC**	TES
45	FTC-dossiernummer 142 3036 Rolnummer C-4459	In de zaak **American Apparel, Inc.**	American Apparel
46	FTC-dossiernummer 142 3026 Rolnummer C-4469	In de zaak **Fantage.com, Inc.**	Fantage
47	FTC-dossiernummer 142 3017 Rolnummer C-4461	In de zaak **Apperian, Inc.**	Apperian
48	FTC-dossiernummer 142 3018 Rolnummer C-4462	In de zaak **Atlanta Falcons Football Club, LLC**	Atlanta Falcons
49	FTC-dossiernummer 142 3019 Rolnummer C-4463	In de zaak **Baker Tilly Virchow Krause, LLP**	Baker Tilly
50	FTC-dossiernummer 142 3020 Rolnummer C-4464	In de zaak **BitTorrent, Inc.**	BitTorrent
51	FTC-dossiernummer 142 3022 Rolnummer C-4465	In de zaak **Charles River Laboratories, Int'l**	Charles River
52	FTC-dossiernummer 142 3023 Rolnummer C-4466	In de zaak **DataMotion, Inc.**	DataMotion
53	FTC-dossiernummer 142 3024 Rolnummer C-4467	In de zaak **DDC Laboratories, Inc.**, handelend onder de naam DNA Diagnostics Center	DDC
54	FTC-dossiernummer 142 3028 Rolnummer C-4470	In de zaak **Level 3 Communications, LLC**	Level 3

55	FTC-dossiernummer 142 3025 Rolnummer C-4468	In de zaak **PDB Sports, Ltd.**, handelend onder de naam the Denver Broncos Football Club, LLP	Broncos
56	FTC-dossiernummer 142 3030 Rolnummer C-4471	In de zaak **Reynolds Consumer Products, Inc.**	Reynolds
57	FTC-dossiernummer 142 3031 Rolnummer C-4472	In de zaak **Receivable Management Services Corporation**	Receivable Mgmt
58	FTC-dossiernummer 142 3032 Rolnummer C-4473	In de zaak **Tennessee Football, Inc.**	Tennessee Football
59	FTC-dossiernummer 102 3058 Rolnummer C-4369	In de zaak **Myspace LLC**	Myspace
60	FTC-dossiernummer 092 3184 Rolnummer C-4365	In de zaak **Facebook, Inc.**	Facebook
61	FTC-dossiernummer 092 3081 Civielrechtelijke vordering nr. 09-CV-5276 (C.D. Cal.)	FTC/Javian Karnani, en **Balls of Kryptonite, LLC**, handelend onder de naam Bite Size Deals, LLC, en Best Priced Brands, LLC	Balls of Kryptonite
62	FTC-dossiernummer 102 3136 Rolnummer C-4336	In de zaak **Google, Inc.**	Google
63	FTC-dossiernummer 092 3137 Rolnummer C-4282	In de zaak **World Innovators, Inc.**	World Innovators
64	FTC-dossiernummer 092 3141 Rolnummer C-4271	In de zaak **Progressive Gaitways LLC**	Progressive Gaitways
65	FTC-dossiernummer 092 3139 Rolnummer C-4270	In de zaak **Onyx Graphics, Inc.**	Onyx Graphics
66	FTC-dossiernummer 092 3138 Rolnummer C-4269	In de zaak **ExpatEdge Partners, LLC**	ExpatEdge
67	FTC-dossiernummer 092 3140 Rolnummer C-4281	In de zaak **Directors Desk LLC**	Directors Desk
68	FTC-dossiernummer 092 3142 Rolnummer C-4272	In de zaak **Collectify LLC**	Collectify

BIJLAGE V

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

6 juli 2023

Commissaris Didier Reynders
Europese Commissie
Wetstraat 200
1049 Brussel
België

Geachte commissaris Reynders,

Het Amerikaanse ministerie van Vervoer (het "ministerie") stelt het op prijs zijn rol bij de handhaving van de beginselen van het EU-VS-kader voor gegevensbescherming ("EU-VS-DPF") te kunnen beschrijven. Het EU-VS-DPF zal een cruciale rol spelen bij de bescherming van persoonsgegevens die bij commerciële transacties worden verstrekt in een wereld waar alles steeds nauwer verweven is. Dankzij het kader kunnen bedrijven belangrijke activiteiten uitvoeren in de wereldeconomie, terwijl tegelijkertijd wordt verzekerd dat consumenten in de EU belangrijke bescherming op het gebied van privacy behouden.

In een brief aan de Europese Commissie van meer dan 22 jaar geleden zegde het ministerie voor het eerst in het openbaar toe te zullen meewerken aan de handhaving van het VS-EU-veiligehavenkader, toezeggingen die werden herhaald en uitgebreid in een brief van 2016 over het EU-VS-privacyschildkader. Het ministerie beloofde in die brieven de VS-EU-veiligehavenbeginselen, en vervolgens de beginselen van het EU-VS-privacyschildkader krachtig te zullen handhaven. Het ministerie breidt deze verbintenis uit tot de beginselen van het EU-VS-DPF en deze brief memoreert die verbintenis.

Het ministerie hernieuwt zijn toezegging in het bijzonder op de volgende cruciale gebieden: 1) het verlenen van prioriteit aan het onderzoek van vermeende schendingen van de EU-VS-DPF-beginselen; 2) passende handhavingsmaatregelen tegen entiteiten die valse of misleidende beweringen doen over deelname aan het EU-VS-DPF; en 3) het houden van toezicht op de uitvoering en de openbaarmaking van handhavingsbevelen inzake schendingen van de EU-VS-DPF-beginselen. We verstrekken hier informatie over elk van deze toezeggingen en, voor de nodige context, tevens achtergrondinformatie over de rol van het ministerie bij de bescherming van de privacy van consumenten en de handhaving van de EU-VS-DPF-beginselen.

1. **Achtergrond**

A. Bevoegdheid van het ministerie op het gebied van privacy

Het ministerie spant zich tot het uiterste in om de privacy te verzekeren inzake informatie die consumenten aan luchtvaartmaatschappijen en reisbureaus verstrekken.

De bevoegdheid van het ministerie om op dit gebied actie te ondernemen, is neergelegd in 49 S.C. § 41712, waarin het luchtvaartmaatschappijen en reisbureaus wordt verboden "oneerlijke of misleidende praktijken uit te voeren" bij luchtvervoer of de verkoop van luchtvervoer. Sectie 41712 volgt hetzelfde patroon als sectie 5 van de Federal Trade Commission (FTC) Act (15 U.S.C. 45).

Onlangs heeft het ministerie voorschriften uitgevaardigd waarin oneerlijke en misleidende praktijken worden gedefinieerd, in overeenstemming met de precedenten van zowel het ministerie als de FTC). Meer in het bijzonder is een praktijk "oneerlijk" wanneer deze consumenten aanzienlijke schade toebrengt of kan toebrengen die door hen redelijkerwijze niet kan worden vermeden en die niet wordt gecompenseerd door voordelen voor de consument of de concurrentie.

Een praktijk is "misleidend" voor consumenten indien zij een onder de gegeven omstandigheden redelijk handelende consument kan misleiden met betrekking tot een wezenlijke kwestie. Een kwestie is van wezenlijk belang als zij het gedrag of de beslissing van de consument met betrekking tot een product of dienst waarschijnlijk heeft beïnvloed. Naast deze algemene beginselen interpreteert het ministerie specifiek sectie 41712 als een verbod voor luchtvaartmaatschappijen en reisbureaus om: 1) de voorwaarden van het eigen privacybeleid te schenden, 2) een door het ministerie uitgevaardigd voorschrift te schenden waarin specifieke privacypraktijken als oneerlijk of misleidend worden aangemerkt; of 3) de Children's Online Privacy Protection Act (wet bescherming online privacy van kinderen, COPPA) of FTC-voorschriften ter uitvoering van de COPPA te schenden; of 4) als deelnemer aan het EU-VS-DPF de beginselen van het EU-VS-DPF niet na te leven ([1]).

Zoals hierboven is opgemerkt, heeft het ministerie op grond van federale wetgeving de exclusieve bevoegdheid om de privacypraktijken van luchtvaartmaatschappijen te reguleren en deelt het rechtsbevoegdheid met de FTC met betrekking tot de privacypraktijken van reisbureaus bij de verkoop van luchtvervoer.

Zodoende kan het ministerie, nadat een luchtvaartmaatschappij of een verkoper van luchtvervoer publiekelijk heeft toegezegd zich te houden aan de beginselen van het EU-VS-DPF, de wettelijke bevoegdheden die zijn vastgesteld in sectie 41712 gebruiken om de naleving van deze beginselen te verzekeren. Zodra een passagier gegevens verstrekt aan een luchtvaartmaatschappij die of reisbureau dat heeft toegezegd zich te zullen houden aan de beginselen van het EU-VS-DPF en dit vervolgens niet doet, handelt deze maatschappij of dit bureau dan ook in strijd met sectie 41712.

B. Handhavingspraktijken

Het Office of Aviation Consumer Protection (bureau voor consumentenbescherming in de luchtvaart, hierna "OACP") ([2]) onderzoekt en vervolgt zaken op grond van 49 U.S.C. § 41712. Het bureau handhaaft het wettelijk verbod in sectie 41712 op oneerlijke en misleidende praktijken voornamelijk door middel van onderhandelingen, het opstellen van administratieve verboden, en het opstellen van besluiten waarin civiele sancties worden beoordeeld. Informatie over mogelijke schendingen verkrijgt het bureau voornamelijk via klachten die worden ingediend door natuurlijke personen, reisbureaus, luchtvaartmaatschappijen en Amerikaanse en buitenlandse overheidsinstanties. Consumenten kunnen de website van het ministerie gebruiken om privacyklachten in te dienen tegen luchtvaartmaatschappijen en reisbureaus. ([3]).

Indien er in een zaak geen redelijke en passende schikking wordt bereikt, heeft het OACP de bevoegdheid om een handhavingsprocedure in te stellen in het kader waarvan een hoorzitting wordt georganiseerd voor een bestuursrechter van het ministerie. Deze rechter heeft de bevoegdheid om administratieve bevelen uit te vaardigen en civiele sancties op te leggen. Een schending van sectie 41712 kan leiden tot een verbod van dergelijke activiteiten en het opleggen van civielrechtelijke sancties tot 37 377 USD voor elke schending van sectie 41712.

Het ministerie heeft geen bevoegdheid om schadevergoeding toe te kennen of geldelijke genoegdoening te bieden aan individuele klagers. Het ministerie heeft echter wel de bevoegdheid om schikkingen goed te keuren naar aanleiding van onderzoek dat is gedaan door het OACP en die rechtstreeks ten gunste komen aan consumenten (bv. contanten, coupons) in plaats van geldboetes die anders aan de Amerikaanse regering zouden moeten worden betaald. Dit is in het verleden voorgekomen en kan ook in het kader van de EU-VS-DPF-beginselen voorkomen, mochten de omstandigheden dat rechtvaardigen. Herhaalde schending van sectie 41712 door een luchtvaartmaatschappij leidt ook tot vragen met betrekking tot de nalevingsbepaling van de maatschappij die, in uitzonderlijke gevallen, ertoe kunnen leiden dat een maatschappij niet langer geschikt voor exploitatie wordt geacht en derhalve haar exploitatievergunning verliest.

Tot op heden heeft het ministerie relatief weinig klachten ontvangen over vermeende privacyschendingen door reisbureaus of luchtvaartmaatschappijen. Als deze zich voordoen, worden ze onderzocht overeenkomstig de voornoemde beginselen.

C. Juridische bescherming door het ministerie ten behoeve van EU-consumenten

Op grond van sectie 41712 is het verbod op oneerlijke of misleidende praktijken in het luchtvervoer of de verkoop van luchtvervoer van toepassing op Amerikaanse en buitenlandse luchtvaartmaatschappijen en reisbureaus. Het ministerie onderneemt regelmatig actie tegen Amerikaanse en buitenlandse luchtvaartmaatschappijen voor praktijken die van invloed zijn op zowel buitenlandse als Amerikaanse consumenten voor zover de praktijken van de luchtvaartmaatschappij plaatsvonden tijdens het bieden van vervoer van en naar de Verenigde Staten. Het ministerie gebruikt alle rechtsmiddelen die het ter beschikking staat om zowel buitenlandse als Amerikaanse consumenten te beschermen tegen oneerlijke en misleidende praktijken in het luchtvervoer door gereguleerde entiteiten en zal dat ook blijven doen.

([1]) https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.
([2]) Voorheen bekend als het Office of Aviation Enforcement and Proceedings.
([3]) http://www.transportation.gov/airconsumer/privacy-complaints.

Het ministerie handhaaft met betrekking tot luchtvaartmaatschappijen tevens andere specifieke wetgeving waarvan de bescherming ook consumenten buiten de VS omvat, zoals de COPPA (wet bescherming online privacy van kinderen). De COPPA verplicht exploitanten van op kinderen gerichte websites en onlinediensten of websites voor het algemene publiek die doelbewust persoonsgegevens verzamelen van kinderen onder de 13 jaar, onder meer om de ouders in kennis te stellen en hun controleerbare toestemming te verkrijgen. Amerikaanse websites en diensten waarop de COPPA van toepassing is en door middel waarvan persoonsgegevens worden verzameld van buitenlandse kinderen, moeten de COPPA in acht nemen. Buitenlandse websites en onlinediensten moeten ook aan de COPPA-bepalingen voldoen als zij gericht zijn op kinderen in de Verenigde Staten of als daarmee doelbewust persoonsgegevens worden verzameld van kinderen in de Verenigde Staten. Voor zover Amerikaanse of buitenlandse luchtvaartmaatschappijen die zaken doen in de VS de COPPA schenden, heeft het ministerie de bevoegdheid om handhavingsmaatregelen te treffen.

II. **Handhaving van de EU-VS-DPF-beginselen**

Als een luchtvaartmaatschappij of reisbureau ervoor kiest deel te nemen aan het EU-VS-DPF en het ministerie een klacht ontvangt dat deze maatschappij of dit bureau de beginselen van het EU-VS-DPF zou hebben geschonden, dan neemt het ministerie de volgende stappen om de beginselen van het EU-VS-DPF krachtig te handhaven.

A. Het geven van prioriteit aan het onderzoek van vermeende schendingen

Het OACP van het ministerie onderzoekt elke klacht waarin wordt gesteld dat de beginselen van het EU-VS-DPF zijn geschonden, waaronder klachten van Europese gegevensbeschermingsautoriteiten en neemt handhavingsmaatregelen wanneer er bewijs is voor de schending.

Daarnaast werkt het OACP samen met de FTC en het ministerie van Handel en geeft het prioriteit aan het onderzoek van beweringen dat de gereguleerde entiteiten zich niet houden aan de toezeggingen inzake privacy die als onderdeel van het EU-VS-DPF zijn gedaan.

Na ontvangst van een beschuldiging van schending van de EU-VS-DPF-beginselen kan het OACP van het ministerie als onderdeel van zijn onderzoek een reeks maatregelen nemen. Het kan bijvoorbeeld het privacybeleid van het reisbureau of de luchtvaartmaatschappij beoordelen, nadere informatie opvragen bij het reisbureau of de luchtvaartmaatschappij of bij derden, de verwijzende entiteit nader raadplegen en beoordelen of er een patroon van schendingen bestaat of sprake is van een aanzienlijk aantal getroffen consumenten. Bovendien stelt het ministerie vast of de kwestie gevolgen heeft voor zaken die binnen de bevoegdheid van het ministerie van Handel of de FTC vallen, beoordeelt het of voorlichting van consumenten of bedrijven nuttig is en begint het, in voorkomend geval, een handhavingsprocedure.

Als het ministerie kennis krijgt van mogelijke schendingen van de EU-VS-DPF-beginselen door reisbureaus, zorgt het voor afstemming dienaangaande met de FTC. Ook informeren we de FTC en het ministerie van Handel over de uitkomst van eventuele handhavingsmaatregelen in het kader van de EU-VS-DPF-beginselen.

B. Aanpak van valse of misleidende verklaringen over deelname

Het ministerie blijft zich inspannen om schendingen van de EU-VS-DPF-beginselen te onderzoeken, waaronder valse of misleidende verklaringen over deelname aan het EU-VS-DPF. We geven prioriteit aan verwijzingen van het ministerie van Handel inzake organisaties waarvan dat ministerie vaststelt dat zij zich ten onrechte uitgeven als deelnemers aan het EU-VS-DPF of dat zij het keurmerk van het EU-VS-DPF zonder toestemming gebruiken.

Daarnaast merken we op dat indien in het kader van het privacybeleid van een organisatie wordt beloofd dat zij de beginselen van het EU-VS-DPF naleeft, het feit dat de organisatie haar zelfcertificering bij het ministerie van Handel niet voltooit of verlengt, op zichzelf allicht geen reden vormt om de organisatie te vrijwaren van de handhaving door het ministerie van Vervoer van deze toezeggingen.

C. Toezicht op uitvoering en openbaarmaking van handhavingsbevelen inzake schendingen van het EU-VS-DPF

Het OACP van het ministerie blijft zich ook inspannen om toezicht te houden op de uitvoering van handhavingsbevelen voor zover dat nodig is om de naleving van de EU-VS-DPF-beginselen te verzekeren. Met name wanneer het bureau een bevel uitvaardigt waarbij een luchtvaartmaatschappij of reisbureau wordt gelast zich in de toekomst te onthouden van schendingen van de EU-VS-DPF-beginselen en sectie 41712 zal het toezicht houden op de naleving door die entiteit van deze verbodsbepaling in het bevel. Daarnaast verzekert het bureau dat besluiten die voortvloeien uit de beginselen van het EU-VS-DPF beschikbaar zijn op zijn website.

We kijken uit naar het voortzetten van de samenwerking met onze federale partners en Europese belanghebbenden op het gebied van het EU-VS-DPF.

Ik hoop u hiermee voldoende te hebben geïnformeerd. Mocht u vragen hebben of meer informatie willen, dan kunt u altijd contact met mij opnemen.

Hoogachtend,

Pete BUTTIGIEG

BIJLAGE VI

Ministerie van Justitie van de Verenigde Staten

Afdeling strafrecht

Bureau van de adjunct-minister van Justitie Washington D.C. 20530

23 juni 2023

Mevrouw Ana Gallego Torres
Directeur-generaal Justitie en consumentenzaken
Europese Commissie
Montoyerstraat 59
1049 Brussel
België

Geachte directeur-generaal Gallego Torres,

Voorts kunnen bedrijven die in de Verenigde Staten gerechtelijk worden vervolgd dit voor de rechter aanvechten, zoals hierna wordt besproken. Van bijzonder belang in het kader van inbeslagneming van gegevens door de overheid is het vierde amendement, dat bepaalt: ([1]) Alle in deze brief beschreven juridische processen zijn niet discriminerend aangezien ze worden gebruikt om gegevens te verkrijgen van bedrijven in de Verenigde Staten, waaronder van bedrijven die zichzelf certificeren overeenkomstig het EU-VS-kader voor gegevensbescherming, ongeacht de nationaliteit of woonplaats van de betrokkene. Voorts kunnen bedrijven die in de Verenigde Staten gerechtelijk worden vervolgd dit voor de rechter aanvechten, zoals hierna wordt besproken ([2]).

Van bijzonder belang in het kader van inbeslagneming van gegevens door de overheid is het vierde amendement, dat bepaalt: „Het recht van de burgers om in hun persoon, huizen, documenten en bezittingen te worden gevrijwaard tegen onredelijke huiszoekingen en inbeslagnemingen, wordt niet geschonden. Slechts op grond van een redelijk vermoeden, gestaafd door eed of stukken, kan een bevel, waarin met name de te doorzoeken plaats en de betrokken personen of de in beslag te nemen goederen worden vermeld, worden afgegeven." Zie U.S. Const. amend. IV. Zoals het Hooggerechtshof van de Verenigde Staten heeft bepaald in Berger v. State of New York: „De belangrijkste doelstelling van dit amendement, zoals is erkend in ontelbare arresten van dit Hof, is het waarborgen van de privacy en veiligheid van personen tegen willekeurige inbreuk door overheidsfunctionarissen.". 388 U.S. 41, 53 (1967) (waarin Camara/Mun. Court of San Francisco, 387 U.S. 523, 528 (1967) wordt aangehaald). In nationale strafrechtelijke onderzoeken verplicht het vierde amendement wetshandhavingsfunctionarissen over het algemeen om een door de rechtbank afgegeven huiszoekingsbevel te verkrijgen voordat zij een doorzoeking verrichten. Zie Katz/United States, 389 U.S. 347, 357 (1967). De normen voor het uitvaardigen van een huiszoekingsbevel, zoals de vereisten inzake redelijk vermoeden en bijzonderheden, zijn van

([1]) In dit overzicht worden niet de onderzoekshulpmiddelen in het kader van de nationale veiligheid beschreven die worden gebruikt door wetshandhavers bij terrorisme en andere onderzoeken in het kader van de nationale veiligheid, waaronder national security letters (NSL's) voor bepaalde gegevens in kredietverslagen, financiële gegevens en elektronische abonnements- en transactiegegevens, 12 U.S. C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 50 U.S.C. § 3162, en voor elektronische surveillance, huiszoekingsbevelen, bedrijfsgegevens en overige verzameling van informatie op grond van de Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 e.v.

([2]) In deze brief worden de federale handhavings- en regelgevingsinstanties besproken. Schendingen van staatswetgeving worden onderzocht door de wetshandhavingsinstanties van de staten en hiervoor wordt geprocedeerd in de staatsrechtbanken. De wetshandhavingsinstanties van de staten maken gebruik van bevelen en dagvaardingen die zijn uitgebracht op grond van de staatswetgeving, in essentie op dezelfde manier als in deze brief is beschreven, maar dan met de mogelijkheid dat het juridische proces in de staat onderworpen kan zijn aan aanvullende waarborgen die zijn opgenomen in de grondwet van de staat of in wetten die verder kunnen gaan dan de waarborgen die zijn opgenomen in de Amerikaanse grondwet. Juridische waarborgen in de staat moeten minimaal gelijk zijn aan de waarborgen in de Amerikaanse grondwet, waaronder, maar niet beperkt tot, het vierde amendement.

toepassing op bevelschriften voor fysieke huiszoekingen en inbeslagnemingen, alsook op bevelschriften voor de opgeslagen inhoud van elektronische communicatie die zijn uitgevaardigd krachtens de Stored Communications Act, zoals hieronder besproken. Als het vereiste van een huiszoekingsbevel niet van toepassing is, zijn activiteiten van de overheid nog steeds onderworpen aan een "redelijkheidstest" op grond van het vierde amendement. Dientengevolge verzekert de grondwet zelf dat de Amerikaanse overheid geen onbeperkte, willekeurige bevoegdheid heeft om privégegevens in beslag te nemen ([3]).

Rechtshandhavingsinstanties:

federale aanklagers, die functionarissen in dienst van het ministerie van Justitie zijn, en federale onderzoeksagenten, waaronder agenten van het Federal Bureau of Investigation (FBI), een wetshandhavingsinstantie binnen het ministerie van Justitie, kunnen de overlegging van documenten en andere gegevens van bedrijven in de Verenigde Staten gelasten ten behoeve van strafrechtelijk onderzoek door middel van meerdere soorten dwingende rechtsfiguren, waaronder dagvaardingen van de kamer van inbeschuldigingstelling, administratieve dwangbevelen en huiszoekingsbevelen, en kunnen andere communicatie verkrijgen op grond van federale bevoegdheden voor afluisteren en nummerregistratie.

Dwangbevelen van de kamer van inbeschuldigingstelling of procesbevelen: strafrechtelijke dwangbevelen worden gebruikt om gerichte wetshandhavingsonderzoeken te ondersteunen. Een dwangbevel van de kamer van inbeschuldigingstelling is een officieel verzoek afkomstig van de kamer van inbeschuldigingstelling (meestal op verzoek van een federale aanklager) om een onderzoek door de kamer van inbeschuldigingstelling uit te voeren naar een specifieke vermeende schending van het strafrecht. De kamer van inbeschuldigingstelling is een onderzoeksafdeling van de rechtbank en de leden ervan worden opgeroepen door een rechter of magistraat. Een dwangbevel kan iemand verplichten te getuigen bij een proces of om bedrijfsgegevens, elektronisch opgeslagen informatie of andere tastbare zaken te overleggen of ter beschikking te stellen. De informatie moet relevant zijn voor het onderzoek en het dwangbevel mag niet onredelijk zijn omdat het te breed is geformuleerd, of omdat het drukkend of belastend is. Een ontvanger kan een motie indienen om een dwangbevel op die gronden aan te vechten. Zie Fed. R. Crim. blz. 17. In beperkte omstandigheden kunnen procesdwangbevelen voor documenten worden gebruikt nadat een zaak door de kamer van inbeschuldigingstelling aanhangig is gemaakt.

Bevoegdheid voor een administratief dwangbevel: de bevoegdheid voor een administratief dwangbevel kan worden uitgeoefend in strafrechtelijke of civiele onderzoeken. In het kader van de handhaving van het strafrecht wordt in meerdere federale wetten de bevoegdheid verleend om administratieve dwangbevelen te gebruiken om bedrijfsgegevens, elektronisch opgeslagen informatie of andere tastbare zaken over te leggen of ter beschikking te stellen die relevant zijn voor onderzoeken betreffende gezondheidszorgfraude, kindermisbruik, bescherming van de geheime dienst, zaken over gecontroleerde stoffen en onderzoeken van de inspecteur-generaal waarbij overheidsinstanties betrokken zijn. Als de overheid een administratief dwangbevel wil gebruiken in de rechtbank, kan de ontvanger van het administratieve dwangbevel, net als de ontvanger van een dwangbevel van de kamer van inbeschuldigingstelling, stellen dat het dwangbevel onredelijk is omdat het te breed geformuleerd is of omdat het drukkend of belastend is.

Gerechtelijke bevelen voor nummerregistratie en traceerapparatuur: op grond van bepalingen in het kader van nummerregistratie en traceerapparatuur kunnen wetshandhavingsinstanties een gerechtelijk bevel verkrijgen om in real time bel-, routing-, adresinformatie en informatie uit berichtenverkeer zonder inhoud te verkrijgen voor een telefoonnummer of e-mailadres na de bevestiging dat de verstrekte informatie relevant is voor een lopend strafrechtelijk onderzoek. Zie 18 U.S.C. §§ 3121-3127. Het gebruik of de installatie van een dergelijk middel zonder toestemming is een federaal misdrijf.

Electronic Communications Privacy Act (ECPA): er zijn aanvullende voorschriften van toepassing op de toegang van de overheid tot abonnee-informatie, verkeersgegevens en opgeslagen inhoud van communicatie in bezit van internetaanbieders (ook gekend als "ISP's"), telefoonbedrijven evenals andere externe dienstverleners, op grond van titel II van de ECPA, ook wel de Stored Communications Act (SCA) genoemd, 18 U.S.C. §§ 2701-2712. In de SCA is een stelsel van wettelijke privacyrechten vastgesteld die de toegang van wetshandhavingsinstanties tot gegevens beperken voor datgene wat in het kader van de grondwet vereist is van klanten en abonnees van internetaanbieders. De SCA voorziet in hogere niveaus van privacywaarborgen, afhankelijk van de indringendheid van de verzameling. Voor het verkrijgen van informatie over abonnees, internetprotocoladressen (IP-adressen) en bijbehorende tijdcodes, evenals van factuurinformatie moeten rechtshandhavingsinstanties een dwangbevel verkrijgen. Voor de meeste andere niet inhoudgerelateerde

([3]) Met betrekking tot de hierboven besproken beginselen van het vierde amendement inzake de bescherming van privacy- en veiligheidsbelangen, passen de Amerikaanse rechters deze beginselen regelmatig toe op nieuwe soorten onderzoekshulpmiddelen die door de ontwikkeling van de technologie mogelijk worden gemaakt. In 2018 oordeelde het Hooggerechtshof bijvoorbeeld dat wanneer de overheid tijdens een rechtshandhavingsonderzoek gedurende een langere periode historische gegevens over de locatie van een mobiele telefoon verwerft die van een mobieletelefoonmaatschappij afkomstig zijn, dit een "huiszoeking" is waarvoor het vierde amendement een bevelschrift vereist. Carpenter/United States, 138 S. Ct. 2206 (2018).

informatie, zoals e-mailheaders zonder onderwerpregel moeten wetshandhavingsinstanties specifieke feiten presenteren aan een rechter waaruit blijkt dat de opgevraagde informatie relevant is en van materieel belang voor een lopend strafrechtelijk onderzoek. Voor het verkrijgen van de opgeslagen inhoud van elektronische communicatie moeten rechtshandhavingsinstanties over het algemeen een huiszoekingsbevel verkrijgen van een rechter op basis van een redelijk vermoeden om aan te nemen dat de desbetreffende account bewijs bevat van een misdrijf. De SCA voorziet tevens in civiele aansprakelijkheid en strafrechtelijke sancties ([4]).

Gerechtelijke bevelen voor surveillance op grond van federale wetgeving inzake afluisteren: daarnaast kunnen wetshandhavingsinstanties mondelinge of elektronische communicatie in real time onderscheppen ten behoeve van strafrechtelijk onderzoek op grond van federale wetgeving inzake afluisteren. Zie 18 U.S.C. §§ 2510-2523. Deze bevoegdheid kan alleen worden uitgeoefend na een gerechtelijk bevel waarin een rechter, onder andere, van mening is dat er gerede aanleiding is om te geloven dat het afluisteren of de elektronische onderschepping bewijs zal opleveren van een federaal misdrijf of de locatie van een voortvluchtige die vervolging ontvlucht. De wet voorziet in civiele aansprakelijkheid en strafrechtelijke sancties voor de schending van de afluisterbepalingen.

Huiszoekingsbevel — Federaal wetboek van strafvordering, regel 41: blz. 41. wetshandhavingsinstanties kunnen elke locatie in de Verenigde Staten fysiek doorzoeken wanneer zij daarvoor toestemming hebben van een rechter. Wetshandhavingsinstanties moeten de rechter ervan overtuigen op basis van een redelijk vermoeden dat er een misdrijf is gepleegd of zal worden gepleegd en dat zaken die verband houden met het misdrijf, waarschijnlijk kunnen worden gevonden op de in het bevel vermelde locatie. Deze bevoegdheid wordt vaak gebruikt wanneer de politie een locatie fysiek moet doorzoeken als gevolg van het risico dat bewijs kan worden vernietigd als een dwangbevel of ander bevel tot overlegging aan het bedrijf wordt betekend. Een persoon die wordt onderworpen aan een zoeking of wiens eigendom wordt doorzocht, kan verzoeken om vernietiging van bewijs dat is verkregen of afgeleid van een onrechtmatige doorzoeking indien dat bewijs tijdens een strafproces tegen die persoon wordt ingebracht. Zie Mapp/Ohio, 367 U.S. 643 (1961). Wanneer een houder van gegevens op grond van een bevel verplicht is gegevens openbaar te maken, kan de gedwongen partij de verplichting tot openbaarmaking met name aanvechten als een te zware last. Zie In re Application of United States, 610 F.2d 1148, 1157 (3d Cir. 1979) (waarin wordt gesteld dat eerlijke rechtsgang vereist dat een hoorzitting wordt gehouden over de kwestie van de last alvorens een telefoonmaatschappij te verplichten bijstand te verlenen bij een huiszoekingsbevel); In re Application of United States, 616 F.2d 1122 (9th Cir. 1980) (komt tot dezelfde conclusie op basis van de toezichthoudende autoriteit van de rechter).

Richtlijnen en beleid van het ministerie van Justitie: In aanvulling op deze grondwettelijke, wettelijke en op regels gebaseerde beperkingen aan de toegang van de overheid tot gegevens, heeft de Attorney General richtsnoeren opgesteld die nadere beperkingen stellen aan de toegang van wetshandhavingsinstanties tot gegevens en die tevens waarborgen omvatten ten aanzien van privacy en burgerlijke vrijheden. Bijvoorbeeld de Attorney General's Guidelines for Domestic FBI Operations (richtsnoeren van de minister van Justitie voor binnenlandse FBI-operaties, hierna "AG FBI Guidelines" genoemd) (september 2008), beschikbaar op http://www.justice.gov/archive/opa/docs/guidelines.pdf, stellen beperkingen vast aan het gebruik van onderzoeksmiddelen om informatie te verkrijgen die verband houdt met onderzoeken inzake federale misdrijven. In deze richtsnoeren wordt de FBI verplicht de minst indringende onderzoeksmethoden te gebruiken, rekening houdend met de gevolgen voor de privacy en burgerlijke vrijheden en mogelijke reputatieschade. Voorts wordt in de richtsnoeren opgemerkt dat het vanzelf spreekt dat de FBI zijn onderzoeken en andere activiteiten op wettige en redelijke manier uitvoert, op een wijze waarbij de vrijheid en de privacy in acht wordt genomen en onnodige indringing in het leven van gezagsgetrouwe personen wordt voorkomen. Zie AG FBI Guidelines, blz. 5. De FBI heeft deze richtsnoeren ten uitvoer gelegd door middel van de *FBI Domestic Investigations and Operations Guide* (FBI-gids voor binnenlandse onderzoeken en operaties, hierna "DIOG"), beschikbaar op https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29, een uitgebreid handboek met gedetailleerde beperkingen aan het gebruik van onderzoeksmiddelen en richtsnoeren om te verzekeren dat de burgerlijke vrijheden en de privacy in elk onderzoek worden beschermd. Aanvullende voorschriften en beleidsmaatregelen waarin beperkingen aan onderzoeksactiviteiten van federale aanklagers zijn vastgesteld, zijn opgenomen in het Justice Manual, dat ook online beschikbaar is op https://www.justice.gov/jm/justicemanual.

Civiele en regelgevende instanties (openbaar belang):

([4]) Bovendien staat sectie 2705, (b) van de SCA de overheid toe een rechterlijk bevel te verkrijgen, op basis van een aangetoonde behoefte aan bescherming tegen openbaarmaking, dat een aanbieder van communicatiediensten verbiedt zijn gebruikers vrijwillig in kennis te stellen van de ontvangst van een dagvaarding uit hoofde van de SCA. In oktober 2017 heeft viceminister van Justitie Rod Rosenstein een memorandum aan de advocaten en vertegenwoordigers van het ministerie van Justitie uitgevaardigd met richtsnoeren om ervoor te zorgen dat verzoeken om dergelijke protective orders ("beschermingsbevelen") zijn toegesneden op de specifieke feiten en aangelegenheden van een onderzoek en met een algemeen plafond van één jaar voor de duur van een verzoek om uitstel van kennisgeving. In mei 2022 publiceerde viceminister van Justitie Lisa Monaco aanvullende richtsnoeren over dit onderwerp, waarin onder meer interne goedkeuringsvereisten van het ministerie van Justitie werden vastgesteld voor verzoeken om een *protective order* te verlengen tot na de oorspronkelijke periode van één jaar en waarin werd bepaald dat *protective orders* aan het einde van een onderzoek moeten worden beëindigd.

Er bestaan ook aanzienlijke beperkingen voor de toegang van civiele of regelgevende instanties (bv. in het openbaar belang) tot gegevens die in bezit zijn van ondernemingen in de Verenigde Staten. Instanties met civiele en regelgevende verantwoordelijkheden kunnen een dagvaarding uitbrengen tegen een onderneming om hun bedrijfsgegevens, elektronisch opgeslagen informatie of andere tastbare zaken op te vragen. Deze instanties kennen beperkingen in de uitoefening van hun bestuurlijke of civiele bevoegdheid voor het uitvaardigen van een dagvaarding, niet alleen door hun organieke statuten, maar ook door onafhankelijke rechterlijke toetsing van dagvaardingen voordat deze mogelijk gerechtelijk worden gehandhaafd. Zie bv. Fed. R. Civ. blz. 45. Instanties mogen alleen toegang vragen tot gegevens die relevant zijn voor zaken die binnen hun regelgevende bevoegdheid vallen. Voorts kan een ontvanger van een administratief dwangbevel de handhaving van dat dwangbevel aanvechten voor de rechter door bewijs te overleggen dat de instantie niet heeft gehandeld in overeenstemming met de basisnormen van redelijkheid, zoals eerder besproken.

Er bestaan andere juridische grondslagen voor bedrijven om verzoeken om gegevens van overheidsinstanties aan te vechten op basis van hun specifieke branche en de soorten gegevens die zij verwerken. Financiële instellingen kunnen bijvoorbeeld administratieve dwangbevelen waarin verzocht wordt om bepaalde soorten informatie, aanvechten vanwege schending van de Bank Secrecy Act en de uitvoeringswetgeving daarvan. 31 U.S.C. § 5318. 31 C.F.R. Hoofdstuk X. Andere bedrijven kunnen een beroep doen op de Fair Credit Reporting Act, U.S.C. § 1681b, of een reeks aan andere sectorspecifieke wetten. Misbruik van de bevoegdheid van een instantie om een dwangbevel uit te vaardigen, kan leiden tot aansprakelijkheid van de instantie of persoonlijke aansprakelijkheid van functionarissen van instanties. Zie bv. Right to Financial Privacy Act, 12 U.S. C. §§ 3401-3423. Rechtbanken in de Verenigde Staten beschermen derhalve tegen onjuiste regelgevende verzoeken en houden onafhankelijk toezicht op de activiteiten van federale instanties.

Tot slot moet elke wettelijke bevoegdheid van administratieve instanties om gegevens van een bedrijf in de Verenigde Staten fysiek in beslag te nemen op grond van een administratieve huiszoeking, voldoen aan de vereisten uit hoofde van het vierde amendement. Zie See/City of Seattle, 387 U.S. 541 (1967).

Conclusie:

alle activiteiten van wetshandhavingsinstanties en regelgevers in de Verenigde Staten moeten voldoen aan de toepasselijke wetgeving, waaronder de Amerikaanse grondwet, wetten, regels en voorschriften. Dergelijke activiteiten moeten tevens voldoen aan de toepasselijke beleidsmaatregelen, waaronder richtsnoeren van de minister van Justitie die van toepassing zijn op de activiteiten van federale wetshandhavers. Het hiervoor beschreven rechtskader beperkt de mogelijkheden van Amerikaanse wetshandhavers en regelgevende instanties om informatie op te vragen bij bedrijven in de Verenigde Staten, ongeacht of deze informatie betrekking heeft op Amerikanen of inwoners van een ander land, en staat daarnaast rechterlijke toetsing toe van overheidsverzoeken om gegevens op grond van deze bevoegdheden.

Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

BIJLAGE VII

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE OFFICE OF GENERAL COUNSEL

WASHINGTON, DC 20511

9 december 2022

Leslie B. Kiernan,
algemeen juridisch adviseur
Ministerie van Handel van de
Verenigde Staten, 1401 Constitution
Ave., NW Washington, DC 20230

Geachte mevrouw Kiernan,

Op 7 oktober 2022 ondertekende president Biden Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities" [Executive Order tot verbetering van de waarborgen voor activiteiten van de VS op het gebied van SIGINT], dat de strenge reeks waarborgen inzake privacy en burgerlijke vrijheden versterkt die van toepassing zijn op Amerikaanse activiteiten op het gebied van SIGINT. Deze waarborgen omvatten: het vereiste dat SIGINT-activiteiten beantwoorden aan opgesomde legitieme doelstellingen; het uitdrukkelijk verbod op dergelijke activiteiten met het oog op specifieke verboden doelstellingen; de invoering van nieuwe procedures om ervoor te zorgen dat de activiteiten op het gebied van SIGINT deze legitieme doelstellingen en geen verboden doelstellingen bevorderen; het vereiste dat activiteiten op het gebied van SIGINT alleen worden uitgevoerd nadat op basis van een redelijke beoordeling van alle relevante factoren is vastgesteld dat de activiteiten noodzakelijk zijn om een gevalideerde inlichtingenprioriteit te bevorderen en alleen in de mate en op een wijze die evenredig is aan de gevalideerde inlichtingenprioriteit waarvoor zij zijn goedgekeurd; en de instructie voor de onderdelen van de inlichtingendiensten om hun beleid en procedures aan te passen aan de in het Executive Order vereiste waarborgen inzake SIGINT. Zeer belangrijk is dat het Executive Order ook een onafhankelijk en bindend mechanisme invoert dat natuurlijke personen uit "in aanmerking komende staten", zoals aangewezen krachtens het Executive Order, in staat stelt verhaal te zoeken indien zij menen te zijn onderworpen aan onwettige activiteiten van de VS op het gebied van SIGINT, met inbegrip van activiteiten die de in het Executive Order vervatte bescherming schenden.

De uitvaardiging door president Biden van Executive Order 14086 was het hoogtepunt van meer dan een jaar van uitvoerige onderhandelingen tussen vertegenwoordigers van de Europese Commissie en de Verenigde Staten en geeft aan welke stappen de Verenigde Staten zullen nemen om hun verbintenissen uit hoofde van het EU-VS-kader voor gegevensbescherming uit te voeren. In overeenstemming met de geest van samenwerking die tot het kader heeft geleid, heb ik begrepen dat u van de Europese Commissie twee reeksen vragen hebt ontvangen over de wijze waarop de inlichtingendiensten het Executive Order zullen uitvoeren. In deze brief ga ik graag op deze vragen in.

Sectie 702 van de Foreign Intelligence Surveillance Act van 1978 (sectie 702 FISA)

De eerste reeks vragen heeft betrekking op sectie 702 FISA, die het mogelijk maakt buitenlandse inlichtingen te verzamelen door niet-Amerikanen van wie redelijkerwijs mag worden aangenomen dat zij zich buiten de Verenigde Staten bevinden, te specificeren als doelwit, met de gedwongen ondersteuning van dienstverleners op het gebied van elektronische communicatie. De vragen betreffen met name de wisselwerking tussen die bepaling en Executive Order 14086, alsmede de andere waarborgen die van toepassing zijn op activiteiten in het kader van sectie 702 FISA.

Om te beginnen kunnen wij bevestigen dat de inlichtingendiensten de waarborgen van Executive Order 14086 zullen toepassen op activiteiten die uit hoofde van sectie 702 FISA worden verricht.

Bovendien gelden er talrijke andere waarborgen voor het gebruik van sectie 702 FISA door de overheid. Zo moeten alle certificeringen uit hoofde van sectie 702 FISA worden ondertekend door zowel de minister van Justitie als de Director of National Intelligence (DNI), en moet de overheid al deze certificeringen ter goedkeuring voorleggen aan de Foreign Intelligence Surveillance Court (FISC), die bestaat uit onafhankelijke rechters die voor het leven zijn benoemd als rechter en die in de FISC een ambtstermijn van zeven jaar vervullen die niet kan worden verlengd. In de certificeringen worden categorieën van te verzamelen buitenlandse inlichtingen vastgesteld, die moeten voldoen aan de wettelijke definitie van buitenlandse inlichtingen, door niet-Amerikanen van wie redelijkerwijs mag worden aangenomen dat zij zich buiten de Verenigde Staten bevinden, als doelwit te specificeren. De certificeringen omvatten informatie over internationaal terrorisme en andere onderwerpen, zoals de verwerving van informatie over massavernietigingswapens. Elke jaarlijkse certificering moet ter goedkeuring aan de FISC worden voorgelegd in een certificeringsaanvraagpakket dat de certificeringen van de minister van Justitie en de DNI bevat, alsmede beëdigde verklaringen van bepaalde hoofden van inlichtingendiensten, en voor de overheid bindende procedures voor het specificeren van doelwitten, minimaliseringsprocedures en procedures voor het doorzoeken. De procedures voor het specificeren van doelwitten vereisen onder meer dat de inlichtingendiensten op basis van het geheel van de omstandigheden redelijkerwijs inschatten dat het specificeren van doelwitten waarschijnlijk zal leiden tot de verzameling van buitenlandse inlichtingen zoals omschreven in een certificering uit hoofde van sectie 702 FISA.

Bovendien moeten de inlichtingendiensten bij het verzamelen van informatie uit hoofde van sectie 702 FISA: een schriftelijke toelichting verstrekken over de basis voor hun beoordeling, op het moment van het specificeren van doelwitten, dat het doelwit naar verwachting in het bezit zal zijn van buitenlandse inlichtingen zoals omschreven in een certificering uit hoofde van sectie 702 FISA, deze naar verwachting zal ontvangen van, of deze waarschijnlijk zal meedelen; bevestigen dat nog steeds wordt voldaan aan de gerichtheidsnorm zoals bepaald in de procedures voor het specificeren van doelwitten uit hoofde van sectie 702 FISA; en de verzameling staken als niet langer aan de norm wordt voldaan. Zie verklaring van de Amerikaanse regering van de Verenigde Staten aan de Foreign Intelligence Surveillance Court,"2015 Summary of Notable Section 702 Requirements" [Samenvatting van de belangrijkste vereisten van sectie 702], blz. 2-3 (15 juli 2015).

Het vereiste dat de inlichtingendiensten hun beoordeling dat de doelwitten uit hoofde van sectie 702 FISA voldoen aan de toepasselijke gerichtheidsnorm, schriftelijk vastleggen en regelmatig bevestigen, vergemakkelijkt het toezicht van de FISC op de activiteiten van de inlichtingendiensten inzake het specificeren van doelwitten. Elke geregistreerde beoordeling en motivering voor het specificeren van doelwitten wordt tweemaandelijks beoordeeld door juristen in het ministerie van Justitie die toezicht houden op de inlichtingendiensten en die dit toezicht onafhankelijk van operaties op het gebied van buitenlandse inlichtingen uitoefenen. De afdeling van het ministerie van Justitie die deze functie vervult, is vervolgens op grond van een reeds lang bestaande regel van de FISC verantwoordelijk voor het melden aan de FISC van schendingen van de toepasselijke procedures. Deze meldingen, samen met regelmatige bijeenkomsten tussen de FISC en deze afdeling van het ministerie van Justitie over het toezicht op de gerichtheidsnorm uit hoofde van sectie 702 FISA, stellen de FISC in staat de naleving van de procedures voor het specificeren van doelwitten en andere procedures uit hoofde van sectie 702 FISA af te dwingen en er anderszins voor te zorgen dat de activiteiten van de overheid rechtmatig zijn. De FISC kan dit met name op een aantal manieren doen, onder meer door bindende corrigerende besluiten uit te vaardigen om de bevoegdheid van de overheid om gegevens over een bepaald doelwit te verzamelen, te beëindigen, of om het verzamelen van gegevens uit hoofde van sectie 702 FISA, te wijzigen of uit te stellen. De FISC kan ook eisen dat de overheid nadere verslagen of briefings verstrekt over de naleving van de procedures voor het specificeren van doelwitten en andere procedures, of eisen dat die procedures worden gewijzigd.

De "bulksgewijze" verzameling van SIGINT

De tweede reeks vragen betreft de "bulksgewijze" verzameling van SIGINT, die in Executive Order 14086 wordt gedefinieerd als de toegestane verzameling van grote hoeveelheden SIGINT die om technische of operationele redenen worden verkregen zonder gebruik van discriminanten (bijvoorbeeld zonder gebruik van specifieke identificatoren of selectietermen).

Met betrekking tot deze vragen merken wij allereerst op dat noch de FISA noch de *national security letters* bulksgewijze verzameling toestaan. Met betrekking tot de FISA:

— titels I en III van de FISA, waarin respectievelijk elektronische surveillance en fysieke zoekopdrachten worden toegestaan, vereisen altijd een gerechtelijk bevel (met beperkte uitzonderingen, bijvoorbeeld in geval van nood) evenals een redelijk vermoeden om aan te nemen dat het doelwit een buitenlandse mogendheid is of een vertegenwoordiger van een buitenlandse mogendheid. Zie 50 U.S.C. §§ 1805, 1824.

— De USA Freedom Act van 2015 wijzigde titel IV van de FISA, die het gebruik van "pen registers en trap and trace devices" (trackers van berichtenverkeer) toestaat, op grond van een rechterlijk bevel (uitgezonderd in geval van nood), om de overheid te verplichten verzoeken te baseren op een "specifieke selectieterm". Zie 50 U.S.C. § 1842(c)(3).

— Titel V van de FISA, die het Federal Bureau of Investigation ("de FBI") toestaat bepaalde soorten bedrijfsgegevens te verkrijgen, vereist een rechterlijk bevel op basis van een verzoek waarin wordt gespecificeerd dat er specifieke en concrete feiten zijn op grond waarvan kan worden aangenomen dat de persoon op wie de gegevens betrekking hebben, een buitenlandse mogendheid of een vertegenwoordiger van een buitenlandse mogendheid is. Zie 50 U.S.C. § 1862(b)(2)(B) ([1]).

— Tot slot laat sectie 702 FISA toe om personen van wie redelijkerwijs wordt aangenomen dat zij zich buiten de Verenigde Staten bevinden, te specificeren als doelwit voor het verwerven van buitenlandse inlichtingen. Zie 50 U.S.C. § 188la, (a). Zoals de Privacy and Civil Liberties Oversight Board heeft opgemerkt, bestaat het verzamelen van gegevens door de regering uit hoofde van sectie 702 FISA, volledig uit het specificeren van individuele personen als doelwitten en het verwerven van communicatie in verband met die personen, van wie de overheid mag verwachten dat zij bepaalde soorten buitenlandse inlichtingen zal verkrijgen, zodat het programma niet werkt door het bulksgewijs verzamelen van communicatie. Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" [Verslag over het surveillanceprogramma uit hoofde van sectie 702 van de Foreign Intelligence Surveillance Act], blz. 103 (2 juli 2014) ([2]).

Met betrekking tot *national security letters* legt de USA FREEDOM Act van 2015 een "specifieke selectieterm" op voor het gebruik van dergelijke *national security letters*. Zie 12 U.S.C. § 3414, (a), (2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v, (a); 18 U.S.C. § 2709, (b).

Voorts is in Executive Order 14086 bepaald dat prioriteit moet worden gegeven aan doelgerichte verzameling en dat, wanneer de inlichtingendiensten overgaan tot het bulksgewijs verzamelen van inlichtingen, de bulksgewijze verzameling van SIGINT alleen wordt toegestaan op basis van de vaststelling dat de informatie die nodig is om een gevalideerde inlichtingenprioriteit te bevorderen, redelijkerwijs niet kan worden verkregen door gerichte verzameling. Zie Executive Order 14086, § 2, (c), (ii), (A).

Wanneer de inlichtingendienst bepaalt dat het bulksgewijs verzamelen aan deze normen voldoet, voorziet Executive Order 14086 bovendien in aanvullende waarborgen. In het bijzonder schrijft het Executive Order voor dat de inlichtingendienst bij het bulksgewijs verzamelen redelijke methoden en technische maatregelen moet toepassen om de verzamelde gegevens te beperken tot wat nodig is om een gevalideerde inlichtingenprioriteit te bevorderen, waarbij het verzamelen van niet-pertinente informatie tot een minimum wordt beperkt. Zie Executive Order 14086. In het Executive Order staat ook dat SIGINT-activiteiten, waaronder het doorzoeken van door middel van bulksgewijs verzamelen verkregen SIGINT, alleen mogen worden uitgevoerd nadat op basis van een redelijke beoordeling van alle relevante factoren is vastgesteld dat de activiteiten noodzakelijk zijn om een gevalideerde inlichtingenprioriteit te bevorderen. Zie Executive Order 14086, § 2, (a), (ii), (A). Het Executive Order geeft verder uitvoering aan dit beginsel door te stellen dat de inlichtingendiensten niet-geminimaliseerde en bulksgewijs verkregen SIGINT alleen mogen doorzoeken ter verwezenlijking van zes toegestane doelstellingen, en dat dergelijke doorzoekingen moeten worden uitgevoerd volgens beleid dat en procedures die op passende wijze rekening houden met de gevolgen van de doorzoekingen voor de privacy en de burgerlijke vrijheden van alle personen, ongeacht hun nationaliteit of de plaats waar zij verblijven. Zie Executive Order 14086, § 2, (c), (iii), (D). Ten slotte voorziet het Executive Order in de behandeling, beveiliging en toegangscontrole van de verzamelde gegevens. Zie Executive Order 14086, § 2, (c), (iii), (A) en § 2, (c), (iii), (B).

* * * * *

Wij hopen dat deze verduidelijkingen nuttig zijn. Aarzel niet om contact met ons op te nemen indien u verdere vragen hebt over de wijze waarop de Amerikaanse inlichtingendiensten voornemens zijn Executive Order 14086 uit te voeren.

([1]) Van 2001 tot 2020 stond titel V van de FISA de FBI toe de FISC om toestemming te vragen voor het verkrijgen van "tastbare zaken" die relevant zijn voor bepaalde toegestane onderzoeken. Zie USA Patriot Act, Pub. L. nr. 107-56, 115 Stat. 272, § 215 (2001). Deze formulering, die is vervallen en dus niet langer de wet is, vormde de bevoegdheid op grond waarvan de overheid ooit bulksgewijs metagegevens over telefonie verzamelde. Nog voordat de bepaling afliep, had de USA Freedom Act haar echter zodanig gewijzigd dat de overheid een verzoek aan de FISC moet baseren op een "specifieke selectieterm". Zie USA Freedom Act, Pub. L. nr. 114-23, 129 Stat. 268, § I 03 (2015).

([2]) De secties 703 en 704, die de inlichtingendiensten machtigen om Amerikaanse personen die zich overzee bevinden als doelwit te specificeren, vereisen een gerechtelijk bevel (uitgezonderd in geval van nood) en altijd een redelijk vermoeden om aan te nemen dat het doelwit een buitenlandse mogendheid, een vertegenwoordiger van een buitenlandse mogendheid of een functionaris of werknemer van een buitenlandse mogendheid is. Zie 50 U.S.C. §§ 1881b, 1881c.

sincerly,

Christopher C. FONZONE
Algemeen juridisch adviseur

BIJLAGE VIII

Lijst van afkortingen

Dit besluit bevat de volgende afkortingen:

AAA	American Arbitration Association
AG Regulation	Regulation on the Data Protection Review Court (Verordening inzake de toetsingsinstantie voor gegevensbescherming) uitgevaardigd door de U.S. Attorney General
AGG-DOM	Richtsnoeren van de minister van Justitie in verband met binnenlandse FBI-operaties
APA	Administrative Procedure Act (wet bestuursrechtelijke procedure)
CIA	Central Intelligence Agency
CNSS	Committee on National Security Systems (comité nationale veiligheidssystemen)
Hof van Justitie	Hof van Justitie van de Europese Unie
Besluit	Uitvoeringsbesluit van de Europese Commissie uit hoofde van Verordening (EU) 2016/679 van het Europees Parlement en de Raad inzake het passende niveau van bescherming van persoonsgegevens krachtens het EU-VS-kader voor gegevensbescherming
DHS	Department of Homeland Security (ministerie van Binnenlandse Veiligheid)
DNI	Director of National Intelligence
DoC	U.S. Department of Commerce (Amerikaans ministerie van Handel)
DoJ	U.S. Department of Justice (Amerikaans ministerie van Justitie)
DoT	U.S. Department of Transportation (Amerikaans ministerie van Vervoer)
DPA	Data Protection Authority (gegevensbeschermingsautoriteit)
DPF-lijst	Lijst van deelnemende organisaties aan het kader voor gegevensbescherming
DPRC	Data Protection Review Court
ECOA	Equal Credit Opportunity Act (wet gelijke kredietkansen)
ECPA	Electronic Communications Privacy Act
EER	Europese Economische Ruimte
EO 12333	Executive Order 12333 United States Intelligence Activities (inlichtingenactiviteiten van de Verenigde Staten)
EO 14086	Executive Order 14086 Enhancing Safeguards for US Signals Intelligence Activities (de waarborgen verbeteren voor activiteiten van de VS op het gebied van signals intelligence)
EU-U.S. DPF of DPF	EU-VS-kader voor gegevensbescherming
EU-U.S. DPF Panel	Panel van het EU-VS-kader voor gegevensbescherming
FBI	Federal Bureau of Investigation
FCRA	Fair Credit Reporting Act (wet billijke kredietrapportage)
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FISCR	Foreign Intelligence Surveillance Court of Review
FOIA	Freedom of Information Act
FRA	Federal Records Act (federale archiefwet)

FTC	U.S. Federal Trade Commission
HIPAA	Health Insurance Portability and Accountability Act (wet overdraagbaarheid en verantwoordingsplicht gezondheidsverzekering)
ICDR	International Centre for Dispute Resolution
IOB	Intelligence Oversight Board (toezichtsraad inzake inlichtingen)
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSL	National Security Letter(s)
ODNI	Office of the Director of National Intelligence
ODNI CLPO, CLPO	Civil Liberties Protection Officer of the Director of National Intelligence
OMB	Office of Management and Budget
OPCL	Office of Privacy and Civil Liberties of the Department of Justice
PCLOB	Privacy and Civil Liberties Oversight Board (raad van toezicht op de privacy en de burgerlijke vrijheden)
PIAB	President's Intelligence Advisory Board (adviesraad van de president inzake inlichtingen)
PPD 28	Presidential Policy Directive 28 (presidentiële beleidsrichtlijn 28)
Verordening (EU) 2016/679	Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.
SAOP	Senior Agency Official for Privacy
De beginselen	Beginselen van het EU-VS-kader voor gegevensbescherming
V.S.	Verenigde Staten
Unie	Europese Unie