II

(Niet-wetgevingshandelingen)

BESLUITEN

UITVOERINGSVERORDENING (EU) 2016/1250 VAN DE COMMISSIE

of 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

(Kennisgeving geschied onder nummer C(2016) 4176)

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens ([1]), en met name artikel 25, lid 6,

Na raadpleging van de Europese Toezichthouder voor gegevensbescherming ([2]),

1. INLEIDING

(1) Richtlijn 95/46/EG bevat de regels voor doorgiften van persoonsgegevens van de lidstaten naar derde landen, voor zover die doorgiften onder het toepassingsgebied daarvan vallen.

(2) Artikel 1 van Richtlijn 95/46/EG en de overwegingen 2 en 10 van de preambule daarvan beogen niet alleen de waarborging van doeltreffende en volledige bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen, met name het grondrecht op eerbiediging van de persoonlijke levenssfeer met betrekking tot de verwerking van persoonsgegevens, maar ook van een hoog niveau van bescherming van die grondrechten en fundamentele vrijheden ([3]).

(3) Het belang van zowel het grondrecht op de eerbiediging van het privéleven, dat wordt gewaarborgd door artikel 7, en het grondrecht op de bescherming van persoonsgegevens, dat wordt gewaarborgd door artikel 8 van het Handvest van de grondrechten van de Europese Unie, wordt benadrukt in de jurisprudentie van het Hof van Justitie ([4]).

(4) Overeenkomstig artikel 25, lid 1, van Richtlijn 95/46/EG moeten de lidstaten bepalen dat persoonsgegevens slechts naar een derde land mogen worden doorgegeven indien dat land een passend beschermingsniveau waarborgt en de wetgeving van de lidstaat die is vastgesteld ter uitvoering van de andere bepalingen van de richtlijn al vóór de doorgifte wordt nageleefd. De Commissie kan vaststellen dat een derde land waarborgen voor een dergelijk passend beschermingsniveau biedt op grond van zijn nationale wetgeving of de internationale verbintenissen die het is aangegaan om de rechten van natuurlijke personen te beschermen. In dat geval, en onverminderd de naleving van de krachtens andere bepalingen van de richtlijn vastgestelde nationale bepalingen, kunnen persoonsgegevens uit de lidstaten worden doorgegeven zonder dat aanvullende waarborgen nodig zijn.

([1]) PB L 281 van 23.11.1995, blz. 31.
([2]) Zie advies 4/2016 over het ontwerp-adequaatheidsbesluit over het EU-VS-privacyschild, gepubliceerd op 30 mei 2016.
([3]) Arrest van het Hof van Justitie van 6 oktober 2015, Schrems, C-362/14, ECLI:EU:C:2015:650, punt 39.
([4]) Arrest van het Hof van Justitie van 7 mei 2009, Rijkeboer, C-553/07, ECLI:EU:C:2009:293, punt 47; arrest van het Hof van Justitie van 8 april 2014, Digital Rights Ireland e.a., gevoegde zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238, punt 53; arrest van het Hof van Justitie van 13 mei 2014, Google Spain en Google, C-131/12, ECLI:EU:C:2014:317, punten 53, 66 en 74.

(5) Overeenkomstig artikel 25, lid 2, van Richtlijn 95/46/EG moet het door een derde land geboden niveau van gegevensbescherming worden beoordeeld met inachtneming van alle omstandigheden die op de doorgifte van gegevens of op een categorie gegevensdoorgiften van invloed zijn, met inbegrip van de algemene en sectoriële rechtsregels die in het betrokken derde land gelden.

(6) In Beschikking 2000/520/EG van de Commissie ([5]) werd voor de toepassing van artikel 25, lid 2, van Richtlijn 95/46/EG vastgesteld dat de „Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer", ten uitvoer gelegd overeenkomstig de richtsnoeren in de „Vaak gestelde vragen" die door het Amerikaanse ministerie van Handel zijn gepubliceerd, werden geacht een passend beschermingsniveau te waarborgen voor persoonsgegevens die uit de Unie worden doorgegeven naar in de Verenigde Staten gevestigde organisaties.

(7) In haar mededelingen COM(2013) 846 final ([6]) en COM(2013) 847 final ([7]) van 27 november 2013 oordeelde de Commissie dat de grondslagen van de veiligehavenregeling moesten worden herzien en versterkt gelet op een aantal factoren, waaronder de exponentiële groei van gegevensstromen en het cruciale belang van die gegevensstromen voor de trans-Atlantische economie, de snelle toename van het aantal Amerikaanse ondernemingen die de veiligehavenregeling onderschrijven en de nieuwe informatie over de omvang en de reikwijdte van bepaalde Amerikaanse inlichtingenprogramma's die vragen doet rijzen over het beschermingsniveau dat de veiligehavenregeling kan waarborgen. Daarnaast heeft de Commissie een aantal tekortkomingen en gebreken in de veiligehavenregeling geconstateerd.

(8) Op basis van het door de Commissie verzamelde bewijsmateriaal, waaronder informatie afkomstig uit de werkzaamheden van de EU-VS-contactgroep inzake privacy ([8]) en de in de ad-hocwerkgroep van de EU en de VS ontvangen informatie over de Amerikaanse inlichtingenprogramma's ([9]), heeft de Commissie 13 aanbevelingen geformuleerd voor een herziening van de veiligehavenregeling. Deze aanbevelingen waren gericht op het versterken van de materiële privacybeginselen, het vergroten van de transparantie van het privacybeleid van de Amerikaanse ondernemingen met een zelfcertificering, beter toezicht en een betere controle en handhaving door de Amerikaanse autoriteiten van de naleving van die beginselen, de beschikbaarheid van betaalbare mechanismen voor geschillenbeslechting en de noodzaak ervoor te zorgen dat de uitzondering inzake de nationale veiligheid waarin Beschikking 2000/520/EG voorziet, slechts wordt ingeroepen voor zover dat strikt noodzakelijk en evenredig is.

(9) In zijn arrest van 6 oktober 2015 in zaak C-362/14, Maximillian Schrems tegen Data Protection Commissioner ([10]), heeft het Hof van Justitie van de Europese Unie Beschikking 2000/520/EG ongeldig verklaard. Zonder onderzoek van de inhoud van de veiligehavenbeginselen oordeelde het Hof dat de Commissie in die beschikking niet had vermeld dat de Verenigde Staten daadwerkelijk „waarborgen boden" voor een passend beschermingsniveau op grond van hun nationale wetgeving of hun internationale verbintenissen ([11]).

(10) In dit verband lichtte het Hof van Justitie toe dat, hoewel de uitdrukking „passend beschermingsniveau" in artikel 25, lid 6, van Richtlijn 95/46/EG niet hetzelfde beschermingsniveau als dat binnen de rechtsorde van de Unie inhoudt, deze zo moet worden opgevat dat wordt vereist dat het derde land een niveau van bescherming van de grondrechten en de fundamentele vrijheden biedt dat „in grote lijnen overeenkomt" met het niveau dat binnen de Unie wordt gewaarborgd op grond van Richtlijn 95/46/EG, gelezen in samenhang met het Handvest van de grondrechten. Ook al kunnen de middelen waarvan dat derde land in dit verband gebruik kan maken, anders zijn dan die welke binnen de Unie worden ingezet, moeten deze middelen in de praktijk niettemin doeltreffend genoeg blijken te zijn ([12]).

(11) Het Hof van Justitie leverde kritiek op het gebrek aan voldoende vaststellingen in Beschikking 2000/520/EG ten aanzien van de vraag of er in de Verenigde Staten overheidsregels bestaan ter beperking van ingrepen in de grondrechten van de personen van wie de gegevens vanuit de Unie naar de Verenigde Staten worden doorgegeven, ingrepen die de overheidsinstanties van dat land mogen verrichten wanneer zij legitieme doelstellingen, zoals de nationale veiligheid, nastreven, en ten aanzien van de vraag of er effectieve rechtsbescherming tegen dat soort ingrepen bestaat ([13]).

([5]) Beschikking 2000/520/EG van de Commissie van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende Vaak gestelde vragen, die door het Amerikaanse ministerie van Handel zijn gepubliceerd (PB L 215 van 28.8.2000, blz. 7).

([6]) Mededeling van de Commissie aan het Europees Parlement en de Raad, Herstel van vertrouwen in de gegevensstromen tussen de EU en de VS, COM(2013) 846 final van 27 november 2013.

([7]) Mededeling van de Commissie aan het Europees Parlement en de Raad betreffende de werking van de veiligehavenregeling („Safe Harbour") uit het oogpunt van EU-burgers en in de EU gevestigde ondernemingen, COM(2013) 847 final van 27 november 2013.

([8]) Zie bv. Raad van de Europese Unie, Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection (eindverslag van de EU-VS-contactgroep op hoog niveau inzake informatie-uitwisseling en privacy en de bescherming van persoonsgegevens), toelichting 9831/08, 28 mei 2008, beschikbaar op het internet op: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf

([9]) Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection (verslag met de bevindingen van de medevoorzitters van de EU over de ad-hocwerkgroep Gegevensbescherming van de EU en de VS), 27 november 2013, beschikbaar op het internet op: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf

([10]) Zie voetnoot 3.

([11]) Arrest Schrems, punt 97.

([12]) Arrest Schrems, punten 73-74.

([13]) Arrest Schrems, punten 88-89.

(12) In 2014 was de Commissie gesprekken aangegaan met de Amerikaanse autoriteiten om de versterking van de veiligehavenregeling overeenkomstig de 13 aanbevelingen in mededeling COM(2013) 847 final te bespreken. Na het arrest van het Hof van Justitie van de Europese Unie in de zaak Schrems zijn deze besprekingen geïntensiveerd om tot een nieuw adequaatheidsbesluit te komen dat voldoet aan de vereisten van artikel 25 van Richtlijn 95/46/EG zoals uitgelegd door het Hof van Justitie. De in de bijlage bij dit besluit opgenomen documenten, die tevens in het Amerikaanse Federal Register zullen worden bekendgemaakt, zijn het resultaat van deze besprekingen. De privacybeginselen (bijlage II) en de in de documenten in de bijlagen I en III tot en met VII opgenomen officiële verklaringen en toezeggingen van verschillende Amerikaanse autoriteiten vormen samen het „EU-VS-privacyschild".

(13) De Commissie heeft de Amerikaanse wetten en praktijken zorgvuldig geanalyseerd, met inbegrip van deze officiële verklaringen en toezeggingen. Op basis van de bevindingen in de overwegingen 136-140 concludeert de Commissie dat door de Verenigde Staten een passend beschermingsniveau wordt gewaarborgd voor persoonsgegevens die in het kader van het EU-VS-privacyschild uit de Unie worden doorgegeven naar organisaties met een zelfcertificering in de Verenigde Staten.

2. **HET „EU-VS-PRIVACYSCHILD"**

(14) Het EU-VS-privacyschild is gebaseerd op een systeem van zelfcertificering waarbij Amerikaanse organisaties een reeks privacybeginselen onderschrijven — de beginselen van het EU-VS-privacyschild, met inbegrip van de Aanvullende Beginselen (hierna samen „de Beginselen" genoemd) — die door het Amerikaanse ministerie van Handel zijn gepubliceerd en in bijlage II bij dit besluit zijn opgenomen. Het geldt zowel voor de verwerkingsverantwoordelijken als voor de verwerkers (vertegenwoordigers), met dien verstande dat verwerkers contractueel ertoe verbonden moeten zijn dat zij slechts volgens instructies van de EU-verwerkingsverantwoordelijke handelen en die laatste bijstaan bij het geven van antwoord aan natuurlijke personen die hun rechten uit hoofde van de Beginselen uitoefenen ([14]).

(15) Onverminderd de naleving van de krachtens Richtlijn 95/46/EG vastgestelde nationale bepalingen, heeft dit besluit het gevolg dat doorgiften van een verwerkingsverantwoordelijke of verwerker in de Unie naar organisaties in de Verenigde Staten die door zelfcertificering bij het ministerie van Handel de Beginselen hebben onderschreven en zich ertoe hebben verbonden die Beginselen na te leven, toegestaan zijn. De Beginselen zijn uitsluitend van toepassing op de verwerking van persoonsgegevens door de Amerikaanse organisatie in zoverre de verwerking door die organisatie niet binnen het toepassingsgebied van de Uniewetgeving valt ([15]). Het privacyschild is niet van invloed op de toepassing van de Uniewetgeving inzake de verwerking van persoonsgegevens in de lidstaten ([16]).

([14]) Zie bijlage II, sectie III.10.a. Overeenkomstig de definitie in sectie I.8.c. zal de EU-verwerker het doel van en de middelen voor de verwerking van de persoonsgegevens bepalen. Voorts moet de overeenkomst met de vertegenwoordiger duidelijk maken of verdere doorgiften toegestaan zijn (zie sectie III.10.a.ii.2.).

([15]) Dit geldt ook wanneer het gaat om personeelsgegevens die uit de Unie worden doorgegeven in het kader van een arbeidsverhouding. Hoewel in de Beginselen de „primaire verantwoordelijkheid" van de EU-werkgever wordt beklemtoond (zie bijlage II, sectie III.9.d.i.), wordt tegelijkertijd daarin duidelijk gemaakt dat zijn gedrag onder de regels zal vallen die in de Unie en/of de respectieve lidstaat van toepassing zijn, en niet onder de Beginselen. Zie bijlage II, sectie III.9.a.i., b.ii., c.i., d.i.

([16]) Dit geldt ook voor verwerking die plaatsvindt met behulp van middelen die zich in de Unie bevinden maar door een buiten de Unie gevestigde organisatie worden gebruikt (zie artikel 4, lid 1, onder c), van Richtlijn 95/46/EG). Vanaf 25 mei 2018 zal de algemene verordening gegevensbescherming van toepassing zijn op de verwerking van persoonsgegevens i) in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie (zelfs wanneer de verwerking plaatsvindt in de Verenigde Staten), of ii) van betrokkenen die zich in de Unie bevinden, door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker, wanneer de verwerking verband houdt met a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist, of b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt. Zie artikel 3, leden 1 en 2, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

(16) De door het privacyschild geboden bescherming van persoonsgegevens geldt voor alle betrokkenen uit de EU ([17]) van wie persoonsgegevens uit de Unie zijn doorgegeven naar organisaties in de VS die door zelfcertificering bij het ministerie van Handel de Beginselen hebben onderschreven.

(17) De Beginselen zijn van toepassing onmiddellijk na de certificering. Er geldt een uitzondering voor het Beginsel van verantwoording voor de verdere doorgifte in het geval een organisatie met een zelfcertificering voor het privacyschild al bestaande commerciële betrekkingen met derden heeft. Omdat het enige tijd kan vergen om die commerciële betrekkingen in overeenstemming te brengen met de regels in het kader van het Beginsel van verantwoording voor de verdere doorgifte, zal de organisatie verplicht zijn om dit zo snel mogelijk te doen doch in elk geval uiterlijk binnen de negen maanden na de zelfcertificering (mits die plaatsvindt in de eerste twee maanden na de dag waarop het privacyschild in werking treedt). In die tussenliggende periode moet de organisatie het Kennisgevingsbeginsel en het Keuzebeginsel toepassen (waardoor de betrokkene uit de EU over een opt-out beschikt); wanneer persoonsgegevens worden doorgegeven aan een derde die als vertegenwoordiger optreedt, moet zij ervoor zorgen dat die laatste ten minste hetzelfde beschermingsniveau biedt als door de Beginselen wordt vereist ([18]). Die overgangsperiode biedt een redelijk en passend evenwicht tussen de eerbiediging van het grondrecht van gegevensbescherming en de legitieme behoefte van ondernemingen aan voldoende tijd om zich aan het nieuwe kader aan te passen wanneer dit ook afhangt van hun commerciële betrekkingen met derden.

(18) Het systeem zal worden beheerd en gecontroleerd door het ministerie van Handel op basis van de toezeggingen die zijn opgenomen in de verklaringen van de Amerikaanse minister van Handel (bijlage I bij dit besluit). Met betrekking tot de handhaving van de Beginselen hebben de Federal Trade Commission (FTC) en het ministerie van Vervoer verklaringen ingediend die zijn opgenomen in bijlage IV en bijlage V bij dit besluit.

2.1. *Privacybeginselen*

(19) Als onderdeel van hun zelfcertificering in het kader van het EU-VS-privacyschild moeten organisaties de toezegging doen dat zij de Beginselen zullen naleven ([19]).

(20) Overeenkomstig het *Kennisgevingsbeginsel* zijn organisaties verplicht de betrokkenen informatie te verschaffen over een aantal belangrijke aspecten van de verwerking van hun persoonsgegevens (bv. de aard van de verzamelde gegevens, het doel van de verwerking, het toegangs- en het keuzerecht, de voorwaarden voor verdere doorgifte en aansprakelijkheid). Er gelden verdere waarborgen, met name de verplichting voor organisaties om hun privacybeleid openbaar te maken (waarin de Beginselen vervat zijn) en te zorgen voor links naar de website van het Amerikaanse ministerie van Handel (met nadere informatie over zelfcertificering, de rechten van betrokkenen en de beschikbare verhaalsmechanismen), de in overweging 30 bedoelde privacyschildlijst en de website van een geschikte alternatieve geschillenbeslechtingsinstantie.

(21) Overeenkomstig het *Beginsel van de integriteit van gegevens en doelbinding* moeten de persoonsgegevens beperkt blijven tot hetgeen relevant is voor het doel van de verwerking, betrouwbaar zijn voor het beoogde gebruik en correct, volledig en actueel zijn. Een organisatie mag geen persoonsgegevens verwerken op een wijze die onverenigbaar is met het doel waarvoor deze oorspronkelijk zijn verzameld of waarmee de betrokkene later heeft ingestemd. Organisaties moeten ervoor zorgen dat persoonsgegevens betrouwbaar zijn voor het geplande gebruik, alsook correct, volledig en actueel.

([17]) 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. De Uniewetgeving inzake gegevensbescherming, waaronder Richtlijn 95/46/EG, valt onder de EER-overeenkomst en is in bijlage XI daarbij opgenomen. Het Gemengd Comité van de EER moet een besluit vaststellen over de opname van dit besluit in de EER-overeenkomst. Zodra dit besluit geldt voor IJsland, Liechtenstein en Noorwegen, zal het EU-privacyschild ook die drie landen dekken en verwijzingen in het privacyschildpakket naar de EU en haar lidstaten worden in die zin gelezen dat ze ook IJsland, Liechtenstein en Noorwegen omvatten.

([18]) Zie bijlage II, sectie III.6.e.

([19]) Er gelden speciale regels om aanvullende waarborgen te bieden voor in het kader van een arbeidsverhouding verzamelde personeelsgegevens zoals vastgesteld in het Aanvullende Beginsel inzake personeelsgegevens van de Beginselen (zie bijlage II, sectie III.9). Zo moeten werkgevers aan de wensen van hun werknemers inzake privacybescherming tegemoetkomen door de toegang tot persoonsgegevens te beperken, sommige gegevens te anonimiseren of codes of pseudoniemen te gebruiken. Bovenal moeten organisaties samenwerken met en gevolg geven aan het advies van de gegevensbeschermingsautoriteiten van de Unie wanneer het om dergelijke gegevens gaat.

(22) Wanneer een nieuw (gewijzigd) doel inhoudelijk verschillend maar nog altijd verenigbaar met het oorspronkelijke doel is, geeft het *Keuzebeginsel* de betrokkenen het recht zich te verzetten (opt-out). Het *Keuzebeginsel* treedt niet in de plaats van het uitdrukkelijke verbod op onverenigbare verwerking ([20]). Voor directe marketing gelden bijzondere regels waardoor een opt-out doorgaans „te allen tijde" mogelijk is voor het gebruik van persoonsgegevens ([21]). In het geval van gevoelige gegevens moeten organisaties normaal gezien de bevestigende toestemming (opt-in) van de betrokkene verkrijgen.

(23) Nog altijd overeenkomstig het *Beginsel van de integriteit van gegevens en doelbinding* mag persoonlijke informatie slechts worden opgeslagen in een vorm die een natuurlijke persoon identificeert of identificeerbaar maakt (en dus in de vorm van persoonsgegevens), zolang dit het doel of de doeleinden dient waarvoor die informatie oorspronkelijk is verzameld of waarmee later is ingestemd. Deze verplichting belet niet dat privacyschildorganisaties 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: archivering in het openbaar belang, journalistiek, literatuur en kunst, wetenschappelijk en historisch onderzoek en statistische analyse. Langere opslag van persoonsgegevens voor een van die doeleinden zal onder de door de Beginselen geboden waarborgen vallen.

(24) Overeenkomstig het *Beveiligingsbeginsel* moeten organisaties die persoonsgegevens verzamelen, bijhouden, gebruiken of verspreiden, „redelijke en passende" beveiligingsmaatregelen nemen, waarbij rekening wordt gehouden met de risico's van de verwerking en de aard van de gegevens. In het geval van subverwerking moeten organisaties met de subverwerker een overeenkomst sluiten die hetzelfde beschermingsniveau garandeert als de Beginselen, en stappen ondernemen om voor de correcte uitvoering daarvan te zorgen.

(25) Overeenkomstig het *Toegangsbeginsel* ([22]) hebben betrokkenen het recht, zonder dat te hoeven rechtvaardigen en uitsluitend tegen een niet buitensporig hoge vergoeding, om van een organisatie antwoord te krijgen op de vraag of deze organisatie hen betreffende persoonsgegevens verwerkt en de gegevens binnen een redelijke termijn meegedeeld te krijgen. Dit recht mag slechts in buitengewone omstandigheden worden beperkt; het weigeren of het beperken van het recht op toegang moet nodig en naar behoren gerechtvaardigd zijn, waarbij de organisatie moet aantonen dat aan deze voorschriften is voldaan. De betrokkenen moeten de persoonlijke informatie, voor zover deze niet correct is of in strijd met de Beginselen is verwerkt, kunnen corrigeren, wijzigen of verwijderen. 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, arbeid), biedt de Amerikaanse wet specifieke bescherming tegen ongunstige beslissingen ([23]). 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. Deze regels bieden bescherming in het waarschijnlijk eerder beperkte aantal gevallen waarin geautomatiseerde beslissingen door de privacyschildorganisatie zelf zouden zijn genomen ([24]). Omdat in de moderne digitale economie steeds meer gebruik wordt gemaakt van geautomatiseerde verwerking (waaronder profiling) als basis voor het nemen van beslissingen die natuurlijke personen betreffen, is dit niettemin een gebied dat van nabij moet worden gevolgd. Om deze controle te faciliteren, is met de Amerikaanse autoriteiten overeengekomen dat een dialoog over geautomatiseerde besluitvorming, met inbegrip van een uitwisseling over de gelijkenissen en de verschillen tussen de aanpak van de EU en de Amerikaanse aanpak, deel zal uitmaken van de eerste jaarlijkse evaluatie en, wanneer nodig, van volgende evaluaties.

([20]) Dit geldt voor alle gegevensdoorgiften in het kader van het privacyschild, ook wanneer het gaat om gegevens die in het kader van een arbeidsverhouding zijn verzameld. Een Amerikaanse organisatie met een zelfcertificering mag 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*. 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.

([21]) Zie bijlage II, sectie III.12.

([22]) Zie ook het Aanvullende Beginsel inzake toegang (bijlage II, sectie III.8).

([23]) 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.).

([24]) In het kader van een doorgifte van persoonsgegevens die in de EU zijn verzameld, zal de contractuele relatie met de natuurlijke persoon (klant) in de meeste gevallen met de EU-verwerkingsverantwoordelijke zijn die de EU-gegevensbeschermingsregels moet naleven, en zullen dus doorgaans alle beslissingen op basis van geautomatiseerde verwerking door hem worden genomen. Dit omvat scenario's waarin de verwerking wordt uitgevoerd door een privacyschildorganisatie die als vertegenwoordiger namens de EU-verwerkingsverantwoordelijke optreedt.

(26) Overeenkomstig het *Beginsel van verhaal, handhaving en aansprakelijkheid* ([25]) moeten de deelnemende organisaties voorzien in solide mechanismen om de naleving van de overige Beginselen te garanderen, alsook in verhaalsmechanismen voor betrokkenen uit de EU van wie persoonsgegevens op niet-conforme wijze zijn verwerkt, met inbegrip van doeltreffende rechtsmiddelen. Zodra een organisatie vrijwillig heeft gekozen voor zelfcertificering ([26]) in het kader van het EU-VS-privacyschild, is zij verplicht de Beginselen daadwerkelijk na te leven. Om voor het ontvangen van persoonsgegevens uit de Unie gebruik te mogen blijven maken van het privacyschild, moet een dergelijke organisatie haar deelname aan het kader jaarlijks opnieuw certificeren. Organisaties moeten ook maatregelen nemen om te controleren ([27]) of hun openbaar gemaakte 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 of steekproefsgewijze controles. Bovendien moet de organisatie een doeltreffend verhaalsmechanisme invoeren voor de behandeling van klachten (zie in dit verband ook overweging 43) en onderworpen zijn aan de onderzoeks- en handhavingsbevoegdheden van de FTC, het ministerie van Vervoer of een andere Amerikaanse overheidsinstantie die gemachtigd is om ervoor te zorgen dat de Beginselen daadwerkelijk worden nageleefd.

(27) Er gelden bijzondere regels voor zogenaamde „verdere doorgiften", d.w.z. doorgiften van persoonsgegevens van een 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. Die regels hebben tot doel ervoor te zorgen dat de bescherming die de persoonsgegevens van betrokkenen uit de EU genieten, niet zal worden ondermijnd noch kan worden omzeild door ze aan derden over te dragen. Dit is bijzonder relevant in complexere verwerkingsketens die typisch zijn voor de digitale economie van vandaag.

(28) Overeenkomstig het *Beginsel van verantwoording voor de verdere doorgifte* ([28]) kunnen verdere doorgiften slechts plaatsvinden i) voor beperkte en welbepaalde doeleinden, ii) op basis van een overeenkomst (of een vergelijkbare regeling binnen een concern ([29])) en iii) uitsluitend indien met die overeenkomst hetzelfde beschermingsniveau wordt geboden als het niveau dat door de Beginselen wordt gewaarborgd, wat het vereiste omvat dat de toepassing van de Beginselen slechts mag worden beperkt in de mate waarin dit nodig is met het oog op de nationale veiligheid, de rechtshandhaving of andere doeleinden van openbaar belang ([30]). Dit moet worden gelezen in samenhang met het *Kennisgevingsbeginsel* en, in het geval van een verdere doorgifte naar een derde-verwerker ([31]), het *Keuzebeginsel*, volgens welke betrokkenen moeten worden geïnformeerd (onder andere) over het soort/de identiteit van derde-ontvangers, het doel van de verdere doorgifte alsook de geboden keuze en zich kunnen verzetten (opt-out) of, in het geval van gevoelige gegevens „uitdrukkelijke bevestigende toestemming" moeten geven (opt-in) voor verdere doorgiften. In het licht van het *Beginsel van de integriteit van gegevens en doelbinding* veronderstelt de verplichting hetzelfde beschermingsniveau te bieden als het niveau dat door de Beginselen wordt gewaarborgd, dat de derde de ontvangen persoonlijke informatie slechts mag verwerken door doeleinden die niet onverenigbaar zijn met de doeleinden waarvoor de persoonlijke informatie oorspronkelijk is verzameld of waarmee de natuurlijke persoon later heeft ingestemd.

(29) 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. In alle gevallen moet de overeenkomst met de derde-ontvanger erin voorzien dat die laatste de privacyschildorganisatie ervan in kennis zal stellen als hij vaststelt dat hij niet langer aan die verplichting kan voldoen. Wanneer een dergelijke vaststelling wordt gedaan, zal de verwerking door de derde worden stopgezet of moeten andere redelijke en passende stappen worden

([25]) Zie ook het Aanvullende Beginsel inzake geschillenbeslechting en handhaving (bijlage II, sectie III.11).
([26]) Zie ook het Aanvullende Beginsel inzake zelfcertificering (bijlage II, sectie III.6).
([27]) Zie ook het Aanvullende Beginsel inzake controle (bijlage II, sectie III.7).
([28]) Zie ook het Aanvullende Beginsel inzake verplichte overeenkomsten voor verdere doorgifte (bijlage II, sectie III.10).
([29]) Zie het Aanvullende Beginsel inzake verplichte overeenkomsten voor verdere doorgifte (bijlage II, sectie III.10.b). Dit beginsel maakt ook doorgiften op basis van niet-contractuele instrumenten (bv. nalevings- en controleprogramma's) 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 Amerikaanse organisatie met een zelfcertificering 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.
([30]) Zie bijlage II, sectie I.5.
([31]) 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.

ondernomen om de situatie te verhelpen ([32]). Wanneer zich in de (sub)verwerkingsketen problemen met de naleving voordoen, zal de privacyschildorganisatie die als de verwerkingsverantwoordelijke van de persoonsgegevens optreedt, moeten aantonen dat zij niet verantwoordelijk is voor de gebeurtenis die de schade heeft veroorzaakt, of anders de aansprakelijkheid moeten aanvaarden, zoals bepaald in het *Beginsel van verhaal, handhaving en aansprakelijkheid*. In het geval van een verdere doorgifte naar een derde-vertegenwoordiger geldt aanvullende bescherming ([33]).

2.2. *Transparantie en beheer van en toezicht op het EU-VS-privacyschild*

(30) Het EU-VS-privacyschild voorziet in toezichts- en handhavingsmechanismen om te controleren en te garanderen dat Amerikaanse ondernemingen met een zelfcertificering de Beginselen naleven en dat tegen een niet-naleving wordt opgetreden. Die mechanismen zijn beschreven in de Beginselen (bijlage II) en de toezeggingen van het ministerie van Handel (bijlage I), de FTC (bijlage IV) en het ministerie van Vervoer (bijlage V).

(31) Voor een correcte toepassing van het EU-VS-privacyschild moeten de belanghebbenden, zoals de betrokkenen, degenen die gegevens naar het buitenland doorgeven en de nationale gegevensbeschermingsautoriteiten kunnen vaststellen welke organisaties de Beginselen onderschrijven. Hiertoe heeft het ministerie van Handel toegezegd een lijst bij te houden en voor het publiek toegankelijk te maken van de organisaties die door zelfcertificering de Beginselen hebben onderschreven en die onder de rechtsbevoegdheid vallen van ten minste een van de in de bijlagen I en II bij dit besluit genoemde handhavingsautoriteiten („de privacyschildlijst") ([34]). Het ministerie van Handel werkt de lijst bij op basis van de jaarlijks doorgegeven hercertificeringen van de organisaties en wanneer een organisatie zich terugtrekt of wordt verwijderd uit het EU-VS-privacyschild. Ook houdt het een officieel register bij van de organisaties die uit de lijst zijn verwijderd en maakt dit voor het publiek toegankelijk, waarbij in elk afzonderlijk geval de reden voor die verwijdering wordt aangegeven. Ten slotte zal het zorgen voor een link naar de lijst van de handhavingszaken van de FTC in verband met het privacyschild, die wordt bijgehouden op de website van de FTC.

(32) Het ministerie van Handel zal zowel de privacyschildlijst als de doorgegeven hercertificeringen bekendmaken via een speciale website. Organisaties met een zelfcertificering moeten op hun beurt het webadres van het ministerie voor de privacyschildlijst verstrekken. Bovendien moet in het privacybeleid van een organisatie, indien dat online beschikbaar is, een link staan naar de website van het privacyschild, alsook een link naar de website of het klachtenformulier van het onafhankelijke verhaalsmechanisme dat beschikbaar is om onopgeloste klachten te onderzoeken. Het ministerie van Handel zal bij de certificering en hercertificering van een organisatie voor het kader systematisch controleren of het privacybeleid overeenstemt met de Beginselen.

(33) Een organisatie wordt in geval van permanente niet-naleving van de Beginselen uit de privacyschildlijst verwijderd en moet de in het kader van het EU-VS-privacyschild ontvangen persoonsgegevens terugbezorgen of wissen. In andere gevallen van verwijdering, zoals vrijwillige terugtrekking van deelname of verzuim de naleving opnieuw te certificeren, mag de organisatie deze gegevens behouden indien 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). In dit geval moet een organisatie een contactpunt binnen de organisatie aanwijzen voor alle vragen in verband met het privacyschild.

(34) Het ministerie van Handel zal toezien op de organisaties die niet langer lid zijn van het EU-VS-privacyschild, hetzij omdat zij zich vrijwillig hebben teruggetrokken hetzij omdat hun certificering is verlopen, om te controleren of zij de eerder op grond van het kader ontvangen persoonsgegevens zullen terugbezorgen, wissen of behouden ([35]). Als de organisaties die gegevens behouden, moeten zij de Beginselen daarop blijven toepassen.

([32]) 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 privacyschildorganisatie — als de verantwoordelijke voor de verwerking door de vertegenwoordiger volgens de gegeven instructies — die stappen ondernemen.

([33]) In een dergelijk geval moet de Amerikaanse organisatie ook 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.

([34]) Informatie over het beheer van de privacyschildlijst kan worden gevonden in bijlage I en bijlage II (sectie I.3, sectie I.4, III.6.d, en sectie III.11.g).

([35]) Zie bv. bijlage II, sectie I.3, sectie III.6.f. en sectie III.11.g.i.

In gevallen waarin het ministerie van Handel organisaties vanwege permanente niet-naleving van de Beginselen uit het kader heeft verwijderd, zal het ervoor zorgen dat die organisaties de op grond van het kader ontvangen persoonsgegevens terugbezorgen of wissen.

(35) Wanneer een organisatie om welke reden dan ook het EU-VS-privacyschild verlaat, moet zij alle openbare verklaringen verwijderen waarmee wordt gesuggereerd dat zij aan het EU-VS-privacyschild blijft deelnemen of recht heeft op de voordelen ervan, met name de verwijzingen naar het EU-VS-privacyschild in haar gepubliceerde privacybeleid. Het ministerie van Handel zal naar valse beweringen aangaande deelname aan het kader, onder meer door voormalige leden, zoeken en daartegen optreden ([36]). 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 (18 U.S.C. § 1001) ([37]).

(36) Het ministerie van Handel zal ambtshalve valse beweringen aangaande deelname aan het privacyschild of het onterechte gebruik van het keurmerk van het privacyschild controleren, en de gegevensbeschermingsautoriteiten kunnen organisaties ter controle verwijzen naar een speciaal contactpunt bij het ministerie. Wanneer een organisatie zich uit het EU-VS-privacyschild heeft teruggetrokken, verzuimt zich opnieuw te certificeren of uit de privacyschildlijst is verwijderd, zal het ministerie van Handel doorlopend controleren of die organisatie uit haar gepubliceerde privacybeleid alle verwijzingen naar het privacyschild waarmee verdere deelname wordt gesuggereerd, heeft verwijderd; indien de organisatie valse beweringen blijft doen, zal het ministerie van Handel de zaak voor mogelijke handhavingsmaatregelen verwijzen naar de FTC, het ministerie van Vervoer of een andere bevoegde autoriteit. Het ministerie van Handel zal ook vragenlijsten toezenden aan organisaties waarvan de zelfcertificering verloopt, of die zich vrijwillig uit het EU-VS-privacyschild hebben teruggetrokken, teneinde te controleren of de organisatie de tijdens haar deelname aan het EU-VS-privacyschild ontvangen persoonsgegevens zal terugbezorgen of wissen, of hierop de Beginselen zal blijven toepassen, en zal, indien de persoonsgegevens worden behouden, controleren wie binnen de organisatie het blijvende contactpunt is voor vragen die met het privacyschild te maken hebben.

(37) Het ministerie van Handel zal doorlopend organisaties met een zelfcertificering aan nalevingscontroles ([38]) onderwerpen, bijvoorbeeld door het toezenden van gedetailleerde vragenlijsten. Het zal tevens systematisch controles verrichten wanneer het een specifieke (ernstige) klacht heeft ontvangen, wanneer een organisatie geen bevredigende antwoorden op vragen geeft of wanneer er betrouwbare aanwijzingen zijn dat een organisatie de Beginselen mogelijk niet naleeft. Waar nodig zal het ministerie van Handel ook overleg plegen met de gegevensbeschermingsautoriteiten over dergelijke nalevingscontroles.

2.3. *Verhaalsmechanismen, behandeling van klachten en handhaving*

(38) Het EU-VS-privacyschild vereist in het *Beginsel van verhaal, handhaving en aansprakelijkheid* dat organisaties natuurlijke personen die door de niet-naleving worden getroffen, verhaalsmechanismen bieden en dus voor betrokkenen uit de EU de mogelijkheid bieden een klacht in te dienen betreffende niet-naleving door Amerikaanse ondernemingen met een zelfcertificering en die klachten opgelost te zien, indien nodig door een beslissing die een doeltreffend herstel biedt.

(39) Als onderdeel van hun zelfcertificering moeten organisaties voldoen aan de vereisten van het Beginsel van verhaal, handhaving en aansprakelijkheid door doeltreffende en direct beschikbare onafhankelijke verhaalsmechanismen 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.

(40) Organisaties mogen onafhankelijke verhaalsmechanismen kiezen in hetzij de Unie hetzij de Verenigde Staten. Dit omvat de mogelijkheid om zich vrijwillig tot samenwerking met de gegevensbeschermingsautoriteiten van de EU

([36]) Zie bijlage I, deel over „zoeken naar en aanpakken van valse beweringen aangaande deelname".
([37]) Zie bijlage II, sectie III.6.h. en sectie III.11.f.
([38]) Zie bijlage I.

te verbinden. Die keuze bestaat echter niet wanneer organisaties personeelsgegevens verwerken, omdat samenwerking met de gegevensbeschermingsautoriteiten dan verplicht is. 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. Organisaties moeten alle problemen van niet-naleving oplossen. Zij moeten ook specificeren dat zij onderworpen zijn aan de onderzoeks- en handhavingsbevoegdheden van de FTC, het ministerie van Vervoer of een andere Amerikaanse overheidsinstantie die gemachtigd is.

(41) Het kader van het privacyschild biedt betrokkenen bijgevolg een aantal mogelijkheden om hun rechten te doen handhaven, klachten in te dienen betreffende niet-naleving door Amerikaanse ondernemingen met een zelfcertificering 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 of bij de FTC.

(42) In gevallen waarin hun klachten niet zijn opgelost door een van deze verhaals- of handhavingsmechanismen, hebben natuurlijke personen ook het recht om bindende arbitrage door het panel van het privacyschild in te roepen (bijlage 1 bij bijlage II van 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 verhaalsmechanismen 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. Er is echter een bepaalde logische volgorde die best wordt gevolgd, zoals hieronder wordt beschreven.

(43) Ten eerste kunnen betrokkenen uit de EU gevallen van niet-naleving van de Beginselen aankaarten via rechtstreekse contacten met de *Amerikaanse onderneming met een zelfcertificering*. Om die klachten gemakkelijk op te lossen, moet de organisatie een doeltreffend verhaalsmechanisme 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 vestigingen in de Unie die op vragen of klachten kunnen reageren) en over de onafhankelijke mechanismen voor de behandeling van klachten.

(44) 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 EU een antwoord geven binnen een termijn van 45 dagen. In dit antwoord moet worden beoordeeld of de klacht gegrond is en informatie worden verstrekt over hoe de organisatie het probleem zal verhelpen. Daarnaast moeten organisaties onmiddellijk reageren op vragen en andere informatieverzoeken van het ministerie van Handel of van een gegevensbeschermingsautoriteit ([39]) (wanneer de organisatie zich verbonden heeft tot samenwerking met de gegevensbeschermingsautoriteiten) betreffende hun naleving van de Beginselen. Organisaties moeten hun informatiebestanden over de uitvoering van hun privacybeleid bewaren en die bij een onderzoek of een klacht wegens niet-naleving op verzoek ter beschikking stellen aan een onafhankelijk verhaalsmechanisme of de FTC (of een andere Amerikaanse autoriteit die bevoegd is om oneerlijke en misleidende praktijken te onderzoeken).

(45) 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. 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. De door een organisatie aangewezen onafhankelijke geschillenbeslechtingsinstanties moeten op hun openbare websites relevante informatie verstrekken over het EU-VS-privacyschild en de diensten die zij in het kader daarvan verlenen. Zij moeten elk jaar een jaarverslag publiceren met daarin geaggregeerde statistieken met betrekking tot deze diensten ([40]).

([39]) 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 II, sectie III.5).

([40]) Het jaarverslag moet het volgende bevatten: 1) het totale aantal tijdens het verslagjaar ontvangen klachten in verband met het privacyschild; 2) de soorten ontvangen klachten; 3) metingen van 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 herstel of opgelegde sancties.

(46) In het kader van zijn nalevingscontroles zal het ministerie van Handel controleren of alle Amerikaanse ondernemingen met een zelfcertificering daadwerkelijk geregistreerd staan bij de onafhankelijke verhaalsmechanismen waarbij zij beweren geregistreerd te staan. Zowel de organisaties als de verantwoordelijke onafhankelijke verhaalsmechanismen moeten onmiddellijk reageren op vragen en informatieverzoeken van het ministerie van Handel in verband met het privacyschild.

(47) 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 oneerlijke en misleidende praktijken te onderzoeken) of een bevoegde rechterlijke instantie van deze niet-naleving in kennis stellen ([41]). 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, zal dit als een permanente niet-naleving worden beschouwd, die ertoe leidt dat het ministerie van Handel de organisatie uit de 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 ([42]). Indien de organisatie na verwijdering uit de lijst blijft beweren dat zij het keurmerk van het privacyschild heeft, zal het ministerie dit verwijzen naar de FTC of een andere handhavingsinstantie ([43]).

(48) Ten derde kunnen natuurlijke personen hun klachten ook indienen bij een *nationale gegevensbeschermingsautoriteit*. 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. 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.

(49) Het advies van de gegevensbeschermingsautoriteiten wordt verstrekt via een informeel panel van gegevensbeschermingsautoriteiten dat op Unieniveau wordt opgericht ([44]), dat zal helpen een geharmoniseerde en samenhangende aanpak van een bepaalde klacht te waarborgen. Het panel zal pas advies uitbrengen 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. 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 op grond van sectie 5 van de FTC Act (of andere soortgelijke wetten). 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 privacyschildlijst wordt verwijderd.

(50) 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 lidstaat.

(51) 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 privacyschildorganisaties 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 ([45]). Ook de FTC heeft toegezegd een specifiek contactpunt in te stellen ([46]) en de gegevensbeschermingsautoriteiten overeenkomstig de Amerikaanse Safe Web Act in onderzoeken bij te staan ([47]).

([41]) Zie bijlage II, sectie III.11.e.
([42]) Zie bijlage II, sectie III.11.g, met name de punten ii) en iii).
([43]) Zie bijlage I, deel over „zoeken naar en aanpakken van valse beweringen aangaande deelname".
([44]) 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.
([45]) Zie bijlage I, delen over het „vergroten van de samenwerking met de gegevensbeschermingsautoriteiten" en het „vergemakkelijken van de afhandeling van klachten over niet-naleving", en bijlage II, sectie II.7.e.
([46]) Zie bijlage IV, blz. 6.
([47]) Ibid.

(52) 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. 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. Om de verwerking van individuele klachten te bespoedigen, zal het contactpunt rechtstreeks contact houden met de respectieve gegevensbeschermingsautoriteit inzake nalevingskwesties en deze in het bijzonder binnen een termijn van ten hoogste 90 dagen na de verwijzing in kennis stellen van de status van klachten. Hierdoor kunnen betrokkenen klachten over niet-naleving door Amerikaanse ondernemingen met een zelfcertificering rechtstreeks bij hun nationale gegevensbeschermingsautoriteit indienen en laten toezenden aan het ministerie van Handel als de Amerikaanse autoriteit die het EU-VS-privacyschild beheert. Het ministerie van Handel heeft ook toegezegd om in de jaarlijkse evaluatie van de werking van het EU-VS-privacyschild een verslag op te nemen waarin de jaarlijks ontvangen klachten in geaggregeerde vorm worden geanalyseerd ([48]).

(53) 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, verwijdert het die organisatie uit de privacyschildlijst. 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.

(54) Ten vijfde moet een privacyschildorganisatie onderworpen zijn aan de onderzoeks- en handhavingsbevoegdheden van de Amerikaanse autoriteiten, met name de *Federal Trade Commission* ([49]), die er daadwerkelijk voor zal zorgen dat de Beginselen worden nageleefd. De FTC zal prioriteit geven 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 ([50]). 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 zal de FTC rechtstreeks door natuurlijke personen ingediende klachten aanvaarden en op eigen initiatief onderzoeken van het privacyschild verrichten, met name als onderdeel van haar ruimere onderzoeken van privacykwesties.

(55) De FTC kan naleving doen handhaven door middel van administratieve bevelen („consent orders") en zal stelselmatig erop toezien dat dergelijke bevelen worden nageleefd. In geval van niet-naleving door organisaties kan de FTC de zaak naar de bevoegde rechterlijke instantie verwijzen om civielrechtelijke sancties en ander herstel te vorderen, onder meer voor door de onrechtmatige gedraging veroorzaakte schade. De FTC kan eventueel ook bij een federale rechterlijke instantie een voorlopige of permanente injunctie of ander herstel vorderen. Elk tegen een privacyschildorganisatie uitgevaardigd consent order zal bepalingen inzake zelfrapportage ([51]) bevatten en organisaties zullen alle relevante delen over het privacyschild van bij de FTC ingediende nalevings- of beoordelingsverslagen openbaar moeten maken. Ten slotte zal de FTC online een lijst bijhouden van de ondernemingen waartegen bevelen van de FTC of een rechterlijke instantie zijn uitgevaardigd in zaken betreffende het privacyschild.

(56) Ten zesde kan de betrokkene uit de EU, als verhaalsmechanisme „in laatste instantie" ingeval zijn klacht door geen van de andere beschikbare verhaalsmechanismen naar tevredenheid is opgelost, bindende arbitrage door het *panel van het privacyschild* inroepen. Organisaties moeten natuurlijke personen informeren over de mogelijkheid om onder bepaalde omstandigheden bindende arbitrage in te roepen en zij moeten reageren zodra een natuurlijke persoon die optie inroept door een kennisgeving aan de betrokken organisatie ([52]).

([48]) Zie bijlage I, deel over „de oplossing van klachten over niet-naleving vergemakkelijken".

([49]) Een privacyschildorganisatie 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.

([50]) 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.

([51]) 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.

([52]) Zie bijlage II, sectie II.1.xi en III.7.c.

(57) Dit arbitragepanel zal bestaan uit een groep van ten minste twintig 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 zullen de partijen uit deze groep een panel van één of drie ([53]) arbiters selecteren. Op de procedure zullen de standaardregels voor arbitrage van toepassing zijn, die door het ministerie van Handel en de Commissie worden overeengekomen. Die regels zullen een aanvulling vormen op het reeds gesloten kader dat verschillende kenmerken heeft waardoor dit mechanisme toegankelijker wordt voor betrokkenen uit de EU: 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 EU 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 ([54]) 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 privacyschildorganisaties worden gestort en waarmee de in aanmerking komende kosten van de arbitrageprocedure worden gedekt tot maximumbedragen die door de Amerikaanse autoriteiten in overleg met de Commissie worden bepaald.

(58) Het panel van het privacyschild zal bevoegd zijn om „individuspecifieke, niet-monetaire billijke schadeloosstelling" ([55]) op te leggen die noodzakelijk is om de niet-naleving van de Beginselen te verhelpen. Hoewel het panel in zijn uitspraak rekening zal houden met het andere herstel dat reeds via andere mechanismen van het privacyschild is verkregen, kunnen natuurlijke personen nog steeds arbitrage inroepen als zij dat andere herstel ontoereikend achten. Hierdoor zullen betrokkenen uit de EU arbitrage kunnen inroepen in alle gevallen waarin hun klachten niet naar tevredenheid zijn opgelost door de maatregelen die 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 Amerikaanse onderneming met een zelfcertificering 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 onderneming de beslissing niet naleeft.

(59) Ten zevende, wanneer een organisatie haar verbintenis de Beginselen en haar openbaar gemaakte privacybeleid na te leven, niet nakomt, zijn er ook nog mogelijkheden om gerechtelijke stappen te ondernemen op grond van de wetgeving van de Amerikaanse staten, bv. rechtsmiddelen in het aansprakelijkheidsrecht, in het geval van bedrieglijke verklaringen, oneerlijke of bedrieglijke handelingen of praktijken, of contractbreuk.

(60) Wanneer een gegevensbeschermingsautoriteit na ontvangst van een klacht van een betrokkene uit de EU van oordeel is dat de doorgifte van de persoonsgegevens van een natuurlijke persoon naar een organisatie in de Verenigde Staten in strijd is met de EU-wetgeving op het gebied van gegevensbescherming, ook wanneer degene die gegevens uit de EU doorgeeft reden heeft om aan te nemen dat de organisatie de Beginselen niet naleeft, kan zij daarnaast haar bevoegdheden ook uitoefenen ten aanzien van degene die gegevens naar het buitenland doorgeeft en, indien nodig, de gegevensdoorgifte opschorten.

(61) In het licht van de informatie in dit deel is de Commissie van oordeel dat de Beginselen die door het Amerikaanse ministerie van Handel zijn gepubliceerd, als zodanig een beschermingsniveau van persoonsgegevens waarborgen dat in grote lijnen overeenkomt met het beschermingsniveau dat wordt gewaarborgd door de in Richtlijn 95/46/EG vastgestelde materiële basisbeginselen.

(62) Daarnaast wordt de daadwerkelijke toepassing van de Beginselen gewaarborgd door de transparantieverplichtingen en het beheer en de nalevingscontroles van het privacyschild door het ministerie van Handel.

(63) Bovendien is de Commissie van oordeel dat, als geheel genomen, de toezichts-, verhaals- en handhavingsmechanismen waarin het privacyschild voorziet, het mogelijk maken om inbreuken op de Beginselen door privacyschildorganisaties in de praktijk vast te stellen en te bestraffen, en de betrokkene rechtsmiddelen bieden om toegang te krijgen tot de hem betreffende persoonsgegevens en, uiteindelijk, om deze gegevens te laten corrigeren of wissen.

([53]) Het aantal arbiters in het panel zal door de partijen worden overeengekomen.

([54]) Het panel kan evenwel oordelen dat dit gelet op de omstandigheden van de specifieke arbitrage tot ongerechtvaardigde of onevenredige kosten zou leiden.

([55]) Natuurlijke personen kunnen in een arbitrageprocedure geen schadevergoeding vorderen, maar als arbitrage wordt ingeroepen, zal de optie om voor de gewone Amerikaanse rechterlijke instanties schadevergoeding te vorderen, blijven bestaan.

3. TOEGANG TOT EN GEBRUIK VAN IN HET KADER VAN HET EU-VS-PRIVACYSCHILD DOORGEGEVEN PERSOONSGEGEVENS DOOR AMERIKAANSE OVERHEIDSDIENSTEN

(64) Zoals volgt uit bijlage II, sectie I.5, wordt de naleving van de Beginselen beperkt in de mate waarin dit nodig is ten behoeve van de nationale veiligheid, het openbaar belang of de rechtshandhaving.

(65) De Commissie heeft een beoordeling verricht van de in de Amerikaanse wetgeving opgenomen beperkingen en waarborgen met betrekking tot de toegang tot en het gebruik van in het kader van het EU-VS-privacyschild doorgegeven persoonsgegevens door Amerikaanse overheidsdiensten ten behoeve van de nationale veiligheid, de rechtshandhaving en andere doeleinden van openbaar belang. Daarnaast heeft de Amerikaanse overheid, via haar Office of the Director of National Intelligence (ODNI) (bureau van de directeur van het nationale inlichtingenwerk) ([56]), de Commissie gedetailleerde verklaringen en toezeggingen verstrekt, die in bijlage VI bij dit besluit zijn opgenomen. In een brief die door de minister van Buitenlandse Zaken is ondertekend, en die in bijlage III bij dit besluit is opgenomen, heeft de Amerikaanse overheid tevens toegezegd een nieuw toezichtsmechanisme voor ingrepen ten behoeve van de nationale veiligheid in het leven te roepen, namelijk de privacyschildombudsman, die onafhankelijk is van de inlichtingendiensten. Ten slotte worden in een in bijlage VII bij dit besluit opgenomen verklaring van het Amerikaanse ministerie van Justitie de beperkingen en waarborgen beschreven met betrekking tot de toegang tot en het gebruik van gegevens door overheidsdiensten ten behoeve van de rechtshandhaving en andere doeleinden van openbaar belang. Met het oog op grotere transparantie en om de wettelijke aard van deze toezeggingen tot uitdrukking te brengen, zullen alle vermelde en bij dit besluit gevoegde documenten in het Federal Register van de Verenigde Staten worden bekendgemaakt.

(66) De bevindingen van de Commissie ten aanzien van de beperkingen van de toegang tot en het gebruik van uit de Europese Unie naar de Verenigde Staten doorgegeven persoonsgegevens door de Amerikaanse overheidsdiensten en het bestaan van doeltreffende rechtsbescherming worden hieronder nader toegelicht.

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

(67) Uit de analyse van de Commissie blijkt dat de Amerikaanse wetgeving een aantal beperkingen bevat met betrekking tot de toegang tot en het gebruik van in het kader van het EU-VS-privacyschild doorgegeven persoonsgegevens ten behoeve van de nationale veiligheid, alsook toezichts- en verhaalsmechanismen die voldoende waarborgen bieden om die gegevens doeltreffend te beschermen tegen onrechtmatige inmenging en het risico van misbruik ([57]). Sinds 2013, toen de Commissie haar twee mededelingen deed (zie overweging 7), is dit rechtskader aanzienlijk versterkt, zoals hieronder wordt beschreven.

3.1.1. Beperkingen

(68) Krachtens de Amerikaanse grondwet valt de waarborging van de nationale veiligheid onder de bevoegdheid van de president als opperbevelhebber van het leger en als hoofd van de uitvoerende macht en, wat betreft buitenlandse inlichtingen, onder zijn bevoegdheid om de buitenlandse zaken van de Verenigde Staten te behartigen ([58]). Hoewel het Congres de bevoegdheid heeft om beperkingen op te leggen, en dit in verschillende opzichten heeft gedaan, kan de president binnen deze grenzen de activiteiten van de Amerikaanse inlichtingendiensten leiden, met name door middel van uitvoeringsbevelen of presidentiële richtlijnen. Dit geldt uiteraard ook op de gebieden waarvoor richtsnoeren van het Congres ontbreken. Momenteel zijn de twee belangrijkste rechtsinstrumenten in dit verband uitvoeringsbevel 12333 (Executive Order 12333, hierna „E.O. 12333" genoemd) ([59]) en presidentiële beleidsrichtlijn 28 (hierna „PPD-28" genoemd).

([56]) De Director of National Intelligence (directeur van het nationale inlichtingenwerk) fungeert als het hoofd van de inlichtingendiensten en treedt op als hoofdadviseur van de president en de National Security Council. Zie de Intelligence Reform and Terrorism Prevention Act van 2004, Pub. L. 108-458 van 17.12.2004. Het ODNI bepaalt onder andere de vereisten voor, en beheert en leidt de taakstelling, verzameling, analyse, productie en verspreiding van nationale inlichtingen door de inlichtingendiensten, onder meer door de ontwikkeling van richtsnoeren voor de wijze waarop informatie of inlichtingen worden geraadpleegd, gebruikt en gedeeld. Zie sectie 1.3 (a), (b) van E.O. 12333.

([57]) Zie arrest Schrems, punt 91.

([58]) Amerikaanse Grondwet, artikel II. Zie ook de inleiding van PPD-28.

([59]) E.O. 12333: United States Intelligence Activities (Uitvoeringsbevel 12333: inlichtingenactiviteiten van de Verenigde Staten), Federal Register vol. 40, nr. 235 (8 december 1981). Voor zover het uitvoeringsbevel openbaar toegankelijk is, bevat het 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 het de algemene parameters voor de uitvoering van inlichtingenactiviteiten vast (met name de noodzaak om specifieke procedureregels af te kondigen). Overeenkomstig punt 3.2 van E.O. 12333 vaardigen de president, ondersteund door de National Security Council, en de Director of National Intelligence de passende richtlijnen, procedures en richtsnoeren uit die nodig zijn om het bevel uit te voeren.

(69) PPD-28 van 17 januari 2014 legt een aantal beperkingen op voor activiteiten met betrekking tot inlichtingen uit berichtenverkeer ([60]). Deze presidentiële beleidsrichtlijn heeft een bindend karakter voor de Amerikaanse inlichtingendiensten ([61]) en blijft van toepassing totdat er een nieuwe Amerikaanse regering aantreedt ([62]). PPD-28 is van bijzonder belang voor niet-Amerikanen, met inbegrip van betrokkenen uit de EU. Daarin is onder meer het volgende bepaald:

a) het verzamelen van inlichtingen uit berichtenverkeer moet gebaseerd zijn op wetten of presidentiële goedkeuring en moet geschieden overeenkomstig de Amerikaanse grondwet (met name het vierde amendement) en de Amerikaanse wetgeving;

b) alle personen moeten met waardigheid en eerbied worden behandeld, ongeacht hun nationaliteit of verblijfplaats;

c) alle personen hebben rechtmatige privacybelangen bij de verwerking van hun persoonsgegevens;

d) de privacy en de burgerlijke vrijheden zijn integrale overwegingen bij de planning van de Amerikaanse activiteiten met betrekking tot inlichtingen uit berichtenverkeer;

e) de Amerikaanse activiteiten met betrekking tot inlichtingen uit berichtenverkeer moeten derhalve voorzien in passende waarborgen voor de persoonsgegevens van alle personen, ongeacht hun nationaliteit of verblijfplaats.

(70) PPD-28 schrijft voor dat het verzamelen van inlichtingen uit berichtenverkeer uitsluitend mag geschieden wanneer de buitenlandse inlichtingen of contraspionage bedoeld zijn ter ondersteuning van nationale en ministeriële opdrachten, en niet voor andere doeleinden (bv. om Amerikaanse ondernemingen een concurrentievoordeel te verschaffen). In dit verband legt het ODNI uit dat de onderdelen van de inlichtingendiensten „waar mogelijk, moeten vereisen dat het verzamelen door middel van discriminanten (bv. specifieke voorzieningen, selectietermen en identificatoren) wordt gericht op specifieke doelwitten of onderwerpen van buitenlandse inlichtingen" ([63]). Voorts bieden de verklaringen de garantie dat besluiten over het verzamelen van inlichtingen niet aan individuele inlichtingenagenten worden overgelaten, maar worden genomen volgens het beleid en de procedures die de verschillende onderdelen van de Amerikaanse inlichtingendiensten (diensten) moeten invoeren voor de uitvoering van PPD-28 ([64]). Het onderzoek naar en de bepaling van passende selectietermen vinden dus plaats binnen het algemene National Intelligence Priorities Framework (NIPF) (nationale kader voor de prioriteiten op het gebied van inlichtingen) dat garandeert dat de prioriteiten met betrekking tot inlichtingen worden vastgesteld door beleidsmakers op hoog niveau en regelmatig worden geëvalueerd om te blijven reageren op reële bedreigingen voor de nationale veiligheid, rekening houdend met mogelijke risico's, waaronder risico's voor de privacy ([65]). Op grond hiervan onderzoekt en bepaalt het personeel van de diensten specifieke selectietermen waarmee naar verwachting buitenlandse inlichtingen worden verzameld die aan de prioriteiten beantwoorden ([66]). De selectietermen („selection terms" of „selectors") moeten regelmatig worden geëvalueerd om na te gaan of ze nog altijd waardevolle inlichtingen opleveren die aan de prioriteiten beantwoorden ([67]).

([60]) Overeenkomstig E.O. 12333 is de directeur van het National Security Agency (de NSA) de functioneel beheerder inzake inlichtingen uit berichtenverkeer en leidt hij een eenvormige organisatie voor activiteiten met betrekking tot inlichtingen uit berichtenverkeer.

([61]) Zie sectie 3.5(h) van E.O. 12333 en voetnoot 1 van PPD-28 voor de definitie van het begrip „Intelligence Community" („inlichtingendiensten").

([62]) Zie het memorandum van het Office of Legal Counsel, ministerie van Justitie, aan president Clinton, 29 januari 2000. Volgens dit juridisch advies hebben presidentiële richtlijnen „dezelfde materiële rechtsgevolgen als een uitvoeringsbevel".

([63]) Verklaringen van het ODNI (bijlage VI), blz. 3.

([64]) Zie sectie 4(b),(c) van PPD-28. Volgens openbare informatie zijn bij de evaluatie van 2015 de huidige zes doeleinden bevestigd. Zie ODNI, Signals Intelligence Reform (Hervorming van de activiteiten met betrekking tot inlichtingen uit berichtenverkeer), voortgangsverslag 2016.

([65]) Verklaringen van het ODNI (bijlage VI), blz. 6 (met verwijzing naar Intelligence Community Directive (ICD) 204). Zie ook sectie 3 van PPD-28.

([66]) Verklaringen van het ODNI (bijlage VI), blz. 6. Zie bijvoorbeeld Civil Liberties and Privacy Office van de NSA, NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333 (Bescherming van de burgerlijke vrijheden en de privacy voor gerichte SIGINT-activiteiten krachtens E.O. 12333 door de NSA), 7 oktober 2014. Zie ook het verslag over de stand van zaken 2014 van het ODNI. Voor verzoeken om toegang op grond van sectie 702 van de FISA zijn zoekopdrachten onderworpen aan de door de FISC goedgekeurde minimaliseringsprocedures. 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.

([67]) Zie Signals Intelligence Reform (Hervorming van de activiteiten met betrekking tot inlichtingen uit berichtenverkeer), jaarverslag 2015. Zie ook de verklaringen van het ODNI (bijlage VI), blz. 6, 8-9, 11.

(71) Voorts blijkt uit de voorschriften in PPD-28, namelijk dat het verzamelen van inlichtingen altijd ([68])„zo specifiek als haalbaar" moet zijn en dat de inlichtingendiensten voorrang moeten geven aan de beschikbaarheid van andere informatie en passende en haalbare alternatieven ([69]), een algemene regel dat gericht verzamelen voorrang moet krijgen boven bulksgewijs verzamelen. Volgens de door het ODNI verstrekte garantie zorgen die voorschriften ervoor dat bulksgewijs verzamelen niet „grootschalig" noch „ongedifferentieerd" is, en dat de uitzondering niet de regel wordt ([70]).

(72) Hoewel in PPD-28 wordt uiteengezet dat de onderdelen van de inlichtingendiensten soms in bepaalde omstandigheden bulksgewijs inlichtingen uit berichtenverkeer moeten verzamelen, bijvoorbeeld om nieuwe of opkomende bedreigingen vast te stellen en te beoordelen, moeten die onderdelen op grond van PPD-28 voorrang geven aan alternatieven die het mogelijk maken gericht inlichtingen uit berichtenverkeer te verzamelen ([71]). Hieruit volgt dat er slechts bulksgewijs zal worden verzameld wanneer gericht verzamelen aan de hand van discriminanten — namelijk een identificator die met een specifiek doelwit geassocieerd is (zoals het e-mailadres of het telefoonnummer van het doelwit) — niet mogelijk is „om technische of operationele redenen" ([72]). Dit geldt zowel voor de manier waarop inlichtingen uit berichtenverkeer worden verzameld als voor wat daadwerkelijk wordt verzameld ([72]).

(73) Volgens de verklaringen van het ODNI zullen de inlichtingendiensten, zelfs wanneer zij geen specifieke identificatoren kunnen gebruiken om gericht te verzamelen, trachten om het verzamelen „zo veel mogelijk" te verengen. Om dit te bewerkstelligen, zullen zij „filters en andere technische hulpmiddelen toepassen om het verzamelen toe te spitsen op die voorzieningen die wellicht communicatieverkeer van buitenlandse inlichtingen van waarde bevatten" (en die beantwoorden aan de vereisten die door de Amerikaanse beleidsmakers zijn geformuleerd volgens de hierboven in overweging 70 beschreven procedure). Het bulksgewijs verzamelen zal hierdoor op ten minste twee manieren gericht gebeuren: om te beginnen zal het altijd betrekking hebben op specifieke doelstellingen op het gebied van buitenlandse inlichtingen (bv. om inlichtingen uit berichtenverkeer te verkrijgen over de activiteiten van een terroristische groepering die in een bepaalde regio actief is) en zich richten op het verzamelen van communicatieverkeer dat daarmee verband houdt. Volgens de door het ODNI verstrekte garantie komt dit tot uiting in het feit dat de „activiteiten van de Verenigde Staten met betrekking tot inlichtingen uit berichtenverkeer slechts een fractie van het communicatieverkeer via het internet treffen" ([73]). Ten tweede wordt in de verklaringen van het ODNI uitgelegd dat de filters en andere gebruikte technische hulpmiddelen zullen worden ontworpen om het verzamelen „zo precies mogelijk" te richten om ervoor te zorgen dat er zo weinig mogelijk „niet-pertinente informatie" wordt verzameld.

(74) Ten slotte beperkt PPD-28, zelfs wanneer de Verenigde Staten het noodzakelijk achten om bulksgewijs inlichtingen uit berichtenverkeer te verzamelen, onder de in de overwegingen 70-73 beschreven voorwaarden het gebruik van dergelijke informatie tot een specifieke lijst van zes doeleinden van nationale veiligheid, zodat de privacy en de burgerlijke vrijheden van alle personen worden beschermd, ongeacht hun nationaliteit en verblijfplaats ([74]). Die toelaatbare doeleinden omvatten maatregelen voor het opsporen en bestrijden van bedreigingen voor de krijgsmacht of het militair personeel die voortkomen uit spionage, terrorisme, bedreigingen voor de cyberveiligheid en massavernietigingswapens, alsook grensoverschrijdende criminele bedreigingen die verband houden met de andere vijf doeleinden, en zullen ten minste jaarlijks worden geëvalueerd. Volgens de verklaringen

([68]) Zie voetnoot 63.

([69]) Ook moet worden opgemerkt dat, overeenkomstig sectie 2.4 van E.O. 12333, de onderdelen van de inlichtingendiensten „de minst ingrijpende verzameltechnieken gebruiken die binnen de Verenigde Staten haalbaar zijn". Wat betreft de beperkingen om alle bulksgewijs verzamelen te vervangen door gericht verzamelen, zie de resultaten van een beoordeling door de National Research Council die zijn opgenomen in het verslag „Surveillance door inlichtingendiensten: waarborging van de grondrechten en rechtsmiddelen in de Europese Unie" van het Bureau van de Europese Unie voor de grondrechten (2015), blz. 18.

([70]) Verklaringen van het ODNI (bijlage VI), blz. 4.

([71]) Zie ook sectie 5(d) van PPD-28, op grond waarvan de Director of National Intelligence, in samenwerking met de hoofden van de betrokken onderdelen van de inlichtingendiensten en het Office of Science and Technology Policy, bij de president een verslag moet indienen „waarin de haalbaarheid wordt beoordeeld van de ontwikkeling van nieuwe software waarmee de inlichtingendiensten gemakkelijker gericht informatie kunnen verzamelen in plaats van bulksgewijs". Volgens openbare informatie luidde de conclusie van dit verslag als volgt: „Er is geen op software gebaseerd alternatief dat een volledige vervanging zal vormen voor bulksgewijs verzamelen bij de opsporing van sommige bedreigingen voor de nationale veiligheid". Zie Signals Intelligence Reform (Hervorming van de activiteiten met betrekking tot inlichtingen uit berichtenverkeer), jaarverslag 2015.

([72]) Zie voetnoot 63.

([73]) Verklaringen van het ODNI (bijlage VI). Dit komt specifiek tegemoet aan de bezorgdheid die de nationale gegevensautoriteiten hadden uitgedrukt in hun advies over het ontwerp-adequaatheidsbesluit. Zie advies 01/2016 van de Artikel 29-werkgroep gegevensbescherming inzake het ontwerpbesluit over de adequaatheid van het Europees-Amerikaanse privacyschild (aangenomen op 13 april 2016), blz. 38 (nr. 47).

([74]) Zie sectie 2 van PPD-28.

van de Amerikaanse overheid hebben de onderdelen van de inlichtingendiensten hun analysepraktijken en normen voor het doorzoeken van onbewerkte inlichtingen uit berichtenverkeer versterkt om aan deze vereisten te voldoen; het gebruik van gerichte zoekopdrachten „waarborgt dat alleen de items waarvan wordt aangenomen dat ze potentieel waardevol zijn voor de inlichtingendienst, voor onderzoek aan de analisten worden voorgelegd" ([75]).

(75) Deze beperkingen zijn van bijzonder belang voor in het kader van het EU-VS-privacyschild doorgegeven persoonsgegevens, met name wanneer het verzamelen van de persoonsgegevens buiten de Verenigde Staten zou plaatsvinden, onder andere tijdens de doorvoer ervan via de trans-Atlantische kabels van de Unie naar de Verenigde Staten. Zoals de Amerikaanse autoriteiten hebben bevestigd in de verklaringen van het ODNI, gelden de daarin opgenomen beperkingen en waarborgen — met inbegrip van die van PPD-28 — voor dergelijke verzameling ([76]).

(76) Zonder als zodanig juridisch geformuleerd te zijn, geven deze beginselen de essentie weer van de beginselen van noodzakelijkheid en evenredigheid. Gericht verzamelen krijgt duidelijk voorrang, terwijl bulksgewijs verzamelen beperkt wordt tot (uitzonderlijke) situaties waarin gericht verzamelen om technische of operationele redenen niet mogelijk is. Zelfs wanneer bulksgewijs verzamelen niet kan worden vermeden, blijft het verdere „gebruik" van dergelijke gegevens *strikt beperkt* tot specifieke legitieme doeleinden van nationale veiligheid ([77]).

(77) Als richtlijn die door de president als hoofd van de uitvoerende macht is uitgevaardigd, zijn deze vereisten bindend voor alle inlichtingendiensten en worden ze verder ten uitvoer gelegd door middel van regels en procedures voor de diensten waarin de algemene beginselen worden omgezet in specifieke aanwijzingen voor de dagelijkse werkzaamheden. Bovendien heeft ook het Congres, hoewel het niet door PPD-28 gebonden is, maatregelen genomen om ervoor te zorgen dat het verzamelen van en de toegang tot persoonsgegevens in de Verenigde Staten niet „algemeen" maar gericht gebeuren.

(78) Uit de beschikbare informatie, met inbegrip van de verklaringen van de Amerikaanse overheid, blijkt dat de Amerikaanse inlichtingendiensten na de doorgifte van de gegevens naar in de Verenigde Staten gevestigde organisaties met een zelfcertificering in het kader van het EU-VS-privacyschild alleen maar ([78]) persoonsgegevens mogen opvragen als hun verzoek voldoet aan de Foreign Intelligence Surveillance Act (FISA) of van het Federal Bureau of Investigation uitgaat op basis van een zogenaamde national security letter (een administratief dwangbevel ten behoeve van de nationale veiligheid) ([79]). De FISA bevat verschillende rechtsgrondslagen die kunnen worden gebruikt om de in het kader van het EU-VS-privacyschild doorgegeven persoonsgegevens van

([75]) Verklaringen van het ODNI (bijlage VI), blz. 4. Zie ook Intelligence Community Directive 203.
([76]) Verklaringen van het ODNI (bijlage VI), blz. 2. Evenzo gelden de in E.O. 12333 vastgestelde beperkingen (bv. dat de verzamelde informatie moet stroken met de door de president vastgestelde prioriteiten met betrekking tot inlichtingen).
([77]) Zie arrest Schrems, punt 93.
([78]) Daarnaast kan het verzamelen van gegevens door de FBI ook gebaseerd zijn op toestemmingen ten behoeve van rechtshandhaving (zie punt 3.2 van dit besluit).
([79]) Zie de verklaringen van het ODNI (bijlage VI), blz. 13-14 en voetnoot 38 voor een nadere toelichting inzake het gebruik van national security letters. Zoals daarin is aangegeven, kan de FBI national security letters alleen gebruiken om niet-inhoudelijke informatie op te vragen die relevant is voor een toegestaan onderzoek op het gebied van de nationale veiligheid ter bescherming tegen internationaal terrorisme of heimelijke inlichtingenactiviteiten. Wat de doorgifte van gegevens in het kader van het EU-VS-privacyschild betreft, lijkt de Electronic Communications Privacy Act (18 U.S.C. § 2709) de voornaamste wettelijke toestemming te zijn, op grond waarvan in elk verzoek om abonnee-informatie of transactiegegevens moet worden gebruikgemaakt van een „term waarmee een persoon, entiteit, telefoonnummer of account specifiek kan worden geïdentificeerd".

betrokkenen uit de EU te verzamelen (en later te verwerken). Naast sectie 104 van de FISA ([80]) met betrekking tot traditionele geïndividualiseerde elektronische surveillance en sectie 402 van de FISA ([81]) met betrekking tot de installatie van „pen registers or trap and trace devices" (trackers van berichtenverkeer), zijn de twee centrale instrumenten sectie 501 van de FISA (voorheen sectie 215 van de USA Patriot Act) en sectie 702 van de FISA ([82]).

(79) In dit verband verbiedt de USA Freedom Act, die op 2 juni 2015 is aangenomen, het bulksgewijs verzamelen van gegevens op basis van sectie 402 van de FISA (bevoegheid inzake trackers van berichtenverkeer), sectie 501 van de FISA (voorheen sectie 215 van de USA Patriot Act) ([83]) en door het gebruik van national security letters; in plaats daarvan moeten specifieke „selectietermen" worden gebruikt ([84]).

(80) Terwijl de FISA verdere wettelijke toestemmingen bevat voor de uitvoering van nationale inlichtingenactiviteiten, waaronder inlichtingen uit berichtenverkeer, is uit de beoordeling van de Commissie gebleken dat, voor zover het om in het kader van het EU-VS-privacyschild door te geven persoonsgegevens gaat, die toestemmingen ook een beperking vormen voor overheidsinmenging ten aanzien van gericht verzamelen en toegang.

(81) Dit is duidelijk voor traditionele geïndividualiseerde elektronische surveillance op grond van sectie 104 van de FISA ([85]). Wat sectie 702 van de FISA betreft, die de basis vormt voor twee belangrijke inlichtingenprogramma's van de Amerikaanse inlichtingendiensten (PRISM en UPSTREAM), worden zoekopdrachten op gerichte wijze uitgevoerd aan de hand van individuele selectietermen waarmee specifieke communicatievoorzieningen worden geïdentificeerd, zoals het e-mailadres of het telefoonnummer van het doelwit, maar niet aan de hand van sleutelwoorden of zelfs de namen van de natuurlijke personen die het doelwit vormen ([86]). Surveillance op grond van sectie 702 bestaat dus, zoals opgemerkt door de Privacy and Civil Liberties Oversight Board (PCLOB), „volledig

([80]) 50 U.S.C. § 1804. Hoewel deze wettelijke bevoegdheid een „uiteenzetting van de door de aanvrager aangevoerde feiten en omstandigheden ter rechtvaardiging van zijn overtuiging dat het doelwit van de elektronische surveillance een buitenlandse mogendheid of een vertegenwoordiger van een buitenlandse mogendheid is" vereist, kan het hierbij 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)). Toch is er slechts een theoretisch verband met in het kader van het EU-VS-privacyschild doorgegeven persoonsgegevens, aangezien de uiteenzetting van de feiten ook de overtuiging moet rechtvaardigen dat „elke voorziening of plaats waarop de elektronische surveillance gericht is, wordt gebruikt, of weldra gaat worden gebruikt, door een buitenlandse mogendheid of een vertegenwoordiger van een buitenlandse mogendheid". In elk geval moet voor het uitoefening van deze bevoegdheid een verzoek worden ingediend bij de FISC, die onder andere zal beoordelen of er op basis van de voorgelegde feiten sprake is van een redelijk vermoeden dat dit inderdaad het geval is.

([81]) 50 U.S.C. § 1842 met § 1841(2) en sectie 3127 van titel 18. 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). Er moet een verzoek om een bevel van de FISC (of een Amerikaanse magistrate judge) worden ingediend en er moet een specifieke selectieterm in de zin van § 1841(4) worden gebruikt, d.w.z. een term waarmee een persoon, account enz. specifiek kan worden geïdentificeerd en die wordt gebruikt om de hoeveelheid opgevraagde informatie zo veel als redelijkerwijs mogelijk is te beperken.

([82]) Terwijl de FBI op grond van sectie 501 van de FISA (voorheen sectie 215 van de USA Patriot Act) bevoegd is om een verzoek om een rechterlijk bevel in te dienen met het oog op de overlegging van „tastbare zaken" (met name telefoonmetagegevens, maar ook bedrijfsgegevens) ten behoeve van buitenlands inlichtingenwerk, kunnen de onderdelen van de Amerikaanse inlichtingendiensten op grond van sectie 702 van de FISA verzoeken om toegang tot informatie indienen, waaronder de inhoud van communicatieverkeer via het internet, vanuit de Verenigde Staten, maar met bepaalde niet-Amerikanen buiten de Verenigde Staten als doelwit.

([83]) Op grond van deze bepaling kan de FBI om „tastbare zaken" vragen (bv. dossiers, papieren, documenten) als aan de FISC wordt aangetoond dat er redelijke gronden zijn om aan te nemen dat die relevant zijn voor een specifiek onderzoek van de FBI. De FBI moet bij de uitvoering van zijn onderzoek door de FISC goedgekeurde selectietermen gebruiken waarvoor een „redelijk, duidelijk vermoeden" bestaat dat een dergelijke term verband houdt met een of meer buitenlandse mogendheden of hun vertegenwoordigers die betrokken zijn bij internationaal terrorisme of activiteiten ter voorbereiding daarvan. Zie Privacy and Civil Liberties Oversight Board, Sec. 215 Report (Verslag over sectie 215), blz. 59; Civil Liberties and Privacy Office van de NSA, Transparency Report: The USA Freedom Act Business Records FISA Implementation (Transparantieverslag: de tenuitvoerlegging van de FISA met betrekking tot bedrijfsgegevens krachtens de USA Freedom Act), 15 januari 2016, blz. 4-6.

([84]) Verklaringen van het ODNI (bijlage VI), blz. 13 (voetnoot 38).

([85]) Zie voetnoot 81.

([86]) Privacy and Civil Liberties Oversight Board, Sec. 702 Report (Verslag over sectie 702), blz. 32-33, met verdere verwijzingen. Volgens zijn Privacy Office moet de NSA 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 tenuitvoerlegging van sectie 702 van de Foreign Intelligence Surveillance Act door de NSA), 16 april 2014.

uit het specificeren als doelwit van specifieke [niet-Amerikaanse] personen over wie een geïndividualiseerd besluit is genomen" ([87]). Als gevolg van een vervalbepaling zal sectie 702 van de FISA in 2017 moeten worden herzien, waarna de Commissie de waarborgen waarover betrokkenen uit de EU beschikken, opnieuw zal moeten beoordelen.

(82) Bovendien heeft de Amerikaanse overheid in haar verklaring de Europese Commissie de uitdrukkelijke garantie gegeven dat de Amerikaanse inlichtingendiensten „niet betrokken zijn bij ongedifferentieerde surveillance op wie dan ook, inclusief gewone Europese burgers" ([88]). Met betrekking tot in de Verenigde Staten verzamelde persoonsgegevens wordt deze verklaring gestaafd met empirisch bewijsmateriaal waaruit blijkt dat *verzoeken om toegang* via national security letters en op grond van de FISA, zowel afzonderlijk als samen, slechts betrekking hebben op een relatief klein aantal doelwitten ten opzichte van de totale gegevensstroom op het internet ([89]).

(83) Wat de *toegang* tot verzamelde gegevens en *gegevensbeveiliging* betreft, schrijft PPD-28 voor dat toegang „is beperkt tot bevoegd personeel dat de informatie nodig heeft om zijn taken te kunnen uitvoeren" en dat persoonsgegevens „op zodanige wijze worden verwerkt en opgeslagen dat passende bescherming wordt geboden en toegang van onbevoegden wordt voorkomen, overeenkomstig de toepasselijke waarborgen voor gevoelige informatie". Het personeel van inlichtingendiensten krijgt een passende en adequate opleiding inzake de beginselen die in PPD-28 zijn vastgelegd ([90]).

(84) Ten slotte staat in PPD-28, met betrekking tot de *opslag* en verdere *verspreiding* van door Amerikaanse inlichtingendiensten verzamelde persoonsgegevens van betrokkenen uit de EU, dat alle personen (inclusief niet-Amerikanen) met waardigheid en eerbied moeten worden behandeld, dat alle personen rechtmatige privacybelangen hebben bij de verwerking van hun persoonsgegevens en dat de onderdelen van de inlichtingendiensten derhalve beleid moeten opstellen dat voorziet in passende waarborgen voor dergelijke gegevens „die de verspreiding en bewaring ervan redelijkerwijs tot een minimum beperken" ([91]).

([87]) Zie Privacy and Civil Liberties Oversight Board, Sec. 702 Report (Verslag over sectie 702), blz. 111. Zie ook de verklaringen van het ODNI (bijlage VI), blz. 9 („Verzameling op grond van sectie 702 van de [FISA] is niet" op grote schaal en ongedifferentieerd„, maar nauw gericht op het verzamelen van buitenlandse inlichtingen van individueel geïdentificeerde legitieme doelwitten") en blz. 13, voetnoot 36 (met verwijzing naar een advies van de FISC van 2014); Civil Liberties and Privacy Office van de NSA, NSA's Implementation of Foreign Intelligence Act Section 702 (De tenuitvoerlegging van sectie 702 van de Foreign Intelligence Surveillance Act door de NSA), 16 april 2014. Zelfs in het geval van UPSTREAM mag de NSA alleen verzoeken om de onderschepping van elektronische communicatie naar, van of over opgegeven selectietermen.

([88]) Verklaringen van het ODNI (bijlage VI), blz. 18. Zie ook blz. 6, waar staat dat de toepasselijke procedures „blijk geven van een duidelijke toezegging om willekeurig en ongedifferentieerd verzamelen van inlichtingen uit berichtenverkeer te voorkomen, en uitvoering te geven — vanaf het hoogste niveau van onze overheid — aan het beginsel van redelijkheid".

([89]) Zie Statistical Transparency Report Regarding Use of National Security Authorities (Statistisch transparantieverslag inzake het gebruik van bevoegdheden op het gebied van de nationale veiligheid), 22 april 2015. Voor de totale stroom van gegevens op het internet, zie bijvoorbeeld Bureau van de Europese Unie voor de grondrechten, Surveillance door inlichtingendiensten: waarborging van de grondrechten en rechtsmiddelen in de Europese Unie, 2015, blz. 15-16. Wat het UPSTREAM-programma betreft, was volgens een vrijgegeven advies van de FISC van 2011 meer dan 90 % van de op grond van sectie 702 van de FISA verkregen elektronische communicatie afkomstig van het PRISM-programma, terwijl minder dan 10 % afkomstig was van het UPSTREAM-programma. Zie FISC, Memorandum Opinion, 2011 WL 10945618 (FISA Ct., 3 oktober 2011), voetnoot 21 (beschikbaar op: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

([90]) Zie sectie 4(a)(ii) van PPD-28. Zie ook ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28 (De bescherming van ieders persoonsgegevens: verslag over de stand van zaken van de ontwikkeling en uitvoering van procedures krachtens PPD-28), juli 2014, blz. 5: „Het beleid van de onderdelen van de inlichtingendiensten moet de bestaande analysepraktijken en normen versterken aan de hand waarvan analisten moeten streven naar structurering van zoekopdrachten of andere zoektermen en technieken om vast te stellen of inlichtingen relevant zijn voor een geldige taak op het gebied van inlichtingen of rechtshandhaving; zoekopdrachten aangaande personen toespitsen op de categorieën inlichtingen die beantwoorden aan een vereiste op het gebied van inlichtingen of rechtshandhaving; en het onderzoek van persoonsgegevens die geen betrekking hebben op vereisten op het gebied van inlichtingen of rechtshandhaving, tot een minimum beperken". Zie bv. CIA, Signals Intelligence Activities (Activiteiten met betrekking tot inlichtingen uit berichtenverkeer), blz. 5; FBI, PPD-28 Policies and Procedures (beleidslijnen en procedures op grond van PPD-28), blz. 3. Volgens het voortgangsverslag 2016 inzake de hervorming van de activiteiten met betrekking tot inlichtingen uit berichtenverkeer hebben de onderdelen van de inlichtingendiensten (waaronder de FBI, de CIA en de NSA) stappen ondernomen om hun personeel bewust te maken van de voorschriften van PPD-28 door een nieuw opleidingsbeleid te ontwikkelen of bestaand opleidingsbeleid aan te passen.

([91]) Volgens de verklaringen van het ODNI gelden deze beperkingen ongeacht of de inlichtingen bulksgewijs of gericht werden verzameld, en ongeacht de nationaliteit van de natuurlijke persoon.

(85) De Amerikaanse overheid heeft uitgelegd dat dit vereiste van redelijkheid betekent dat de onderdelen van de inlichtingendiensten niet „elke theoretisch mogelijke maatregel" zullen hoeven te nemen, maar dat zij „hun inspanningen ter bescherming van de rechtmatige belangen op het gebied van privacy en burgerlijke vrijheden in evenwicht zullen moeten brengen met de praktische vereisten van activiteiten met betrekking tot inlichtingen uit berichtenverkeer" ([92]). In dit verband zullen niet-Amerikanen op dezelfde wijze worden behandeld als Amerikanen, op basis van door de Attorney General goedgekeurde procedures ([93]).

(86) Volgens deze regels is de bewaring doorgaans beperkt tot een maximum van vijf jaar, tenzij er een specifieke wettelijke bepaling is of een uitdrukkelijk besluit van de Director of National Intelligence na een zorgvuldige evaluatie van privacyaspecten — waarbij rekening wordt gehouden met de standpunten van de Civil Liberties Protection Officer (functionaris voor de bescherming van de burgerlijke vrijheden) van het ODNI en de functionarissen voor de burgerlijke vrijheden en de privacy van de diensten — dat voortdurende bewaring in het belang van de nationale veiligheid is ([94]). De verspreiding is beperkt tot gevallen waarin de informatie relevant is voor het onderliggende doel van het verzamelen en derhalve beantwoordt aan een toegestaan vereiste op het gebied van buitenlandse inlichtingen of rechtshandhaving ([95]).

(87) Volgens de door de Amerikaanse overheid gegeven garanties mogen persoonsgegevens niet worden verspreid louter omdat de betrokken natuurlijke persoon geen Amerikaan is, en „worden inlichtingen uit berichtenverkeer met betrekking tot de routineactiviteiten van een buitenlandse persoon niet beschouwd als buitenlandse inlichtingen die kunnen worden verspreid of permanent bewaard op grond van dat loutere feit, tenzij die op andere wijze beantwoorden aan een toegestaan vereiste op het gebied van buitenlandse inlichtingen" ([96]).

(88) Op basis van al het bovenstaande concludeert de Commissie dat er in de Verenigde Staten regelgeving bestaat die bedoeld is om ingrepen ten behoeve van de nationale veiligheid in de grondrechten van de personen van wie persoonsgegevens uit de Unie naar de Verenigde Staten worden doorgegeven in het kader van het EU-VS-privacyschild, te beperken tot hetgeen strikt noodzakelijk is om het betrokken legitieme doel te bereiken.

(89) Zoals uit bovenstaande analyse blijkt, garandeert de Amerikaanse wetgeving dat surveillancemaatregelen slechts zullen worden genomen om buitenlandse inlichtingen te verkrijgen — wat een legitieme beleidsdoelstelling is ([97]) — en zo specifiek mogelijk zullen zijn. Bulksgewijs verzamelen zal met name alleen uitzonderlijk worden

([92]) Zie de verklaringen van het ODNI (bijlage VI).

([93]) Zie sectie 4(a)(i) van PPD-28 met sectie 2.3 van E.O. 12333.

([94]) Sectie 4(a)(i) van PPD-28; verklaringen van het ODNI (bijlage VI), blz. 7. Met betrekking tot op grond van sectie 702 van de FISA verzamelde persoonsgegevens voorzien de door de FISC goedgekeurde minimaliseringsprocedures van de NSA er bijvoorbeeld als regel in dat de metagegevens en onbewerkte inhoud voor PRISM niet langer dan vijf jaar worden bewaard, terwijl de gegevens voor UPSTREAM niet langer dan twee jaar worden bewaard. De NSA voldoet aan deze beperkingen voor de bewaring via een geautomatiseerd proces dat de verzamelde gegevens aan het einde van de respectieve bewaartermijn wist. Zie NSA, Sec. 702 FISA Minimization Procedures (De minimaliseringsprocedures op grond van sectie 702 van de FISA), sectie 7 met sectie 6(a)(1); 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. Evenzo is de bewaring op grond van sectie 501 van de FISA (voorheen sectie 215 van de USA Patriot Act) beperkt tot vijf jaar, tenzij de persoonsgegevens deel uitmaken van naar behoren goedgekeurde verspreiding van buitenlandse inlichtingen, of het ministerie van Justitie de NSA er schriftelijk van op de hoogte brengt dat voor de gegevens een bewaarverplichting geldt in hangende of verwachte rechtszaken. Zie Civil Liberties and Privacy Office van de NSA, Transparency Report: The USA Freedom Act Business Records FISA Implementation (Transparantieverslag: de tenuitvoerlegging van de FISA met betrekking tot bedrijfsgegevens krachtens de USA Freedom Act), 15 januari 2016.

([95]) In het bijzonder mogen persoonsgegevens, in geval van sectie 501 van de FISA (voorheen sectie 215 van de USA Patriot Act), uitsluitend worden verspreid om terrorisme te bestrijden of als bewijs van een misdaad; in geval van sectie 702 van de FISA mag dit uitsluitend als er een geldige reden is in verband met buitenlandse inlichtingen of rechtshandhaving. 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; Transparency Report: The USA Freedom Act Business Records FISA Implementation (Transparantieverslag: de tenuitvoerlegging van de FISA met betrekking tot bedrijfsgegevens krachtens de USA Freedom Act), 15 januari 2016. Zie ook NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333 (Bescherming van de burgerlijke vrijheden en de privacy voor gerichte SIGINT-activiteiten krachtens E.O. 12333 door de NSA), 7 oktober 2014.

([96]) Verklaringen van het ODNI (bijlage VI), blz. 7 (met verwijzing naar de Intelligence Community Directive 203).

([97]) Het Hof van Justitie heeft verduidelijkt dat de nationale veiligheid een legitieme beleidsdoelstelling is. Zie arrest Schrems, punt 88. Zie ook arrest Digital Rights Ireland e.a., punten 42-44 en 51, waarin het Hof van Justitie heeft geoordeeld dat de doeltreffendheid van de bestrijding van zware criminaliteit, met name van georganiseerde misdaad en terrorisme, in aanzienlijke mate kan afhangen van het gebruik van moderne onderzoekstechnieken. Bovendien zijn inlichtingenactiviteiten, anders dan strafrechtelijke onderzoeken waarbij het er doorgaans om gaat achteraf te bepalen wie de verantwoordelijkheid en de schuld draagt voor gedragingen in het verleden, vaak gericht op het voorkomen van bedreigingen voor de nationale veiligheid voordat schade wordt berokkend. Dergelijke onderzoeken kunnen dus vaak een ruimere reeks mogelijke actoren („doelwitten") en een ruimer geografisch gebied betreffen. Zie arrest van het Europees Hof voor de rechten van de mens van 29 juni 2006, Weber en Saravia/Duitsland, verzoekschrift nr. 54934/00, punten 105-118 (inzake de zogenaamde „strategische monitoring").

toegestaan wanneer gericht verzamelen niet haalbaar is, en zal vergezeld gaan van aanvullende waarborgen om de hoeveelheid verzamelde gegevens en de daaropvolgende toegang (die gericht zal moeten zijn en alleen voor specifieke doeleinden toegestaan is) zo veel mogelijk te beperken.

(90) Volgens de beoordeling van de Commissie voldoet dit aan de norm die door het Hof van Justitie in het arrest Schrems is vastgesteld, namelijk dat wetgeving die een inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten met zich brengt, „minimale vereisten" ([98]) moet opleggen, en dat „wetgeving die algemeen toestaat dat alle persoonsgegevens van alle personen van wie de gegevens vanuit de Unie naar de Verenigde Staten worden doorgegeven, worden bewaard, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het nagestreefde doel en zonder dat wordt voorzien in een objectief criterium ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan voor specifieke doeleinden, die strikt beperkt zijn en als rechtvaardiging kunnen dienen voor de inmenging als gevolg van zowel de toegang tot als het gebruik van deze gegevens, niet beperkt tot het strikt noodzakelijke is" ([99]). Evenmin zal er onbeperkte verzameling en opslag van gegevens van alle personen zonder beperkingen zijn, noch onbeperkte toegang. Bovendien sluiten de aan de Commissie verstrekte verklaringen, met inbegrip van de garantie dat de Amerikaanse activiteiten met betrekking tot inlichtingen uit berichtenverkeer slechts een fractie van het communicatieverkeer via het internet treffen, uit dat er „op veralgemeende basis" ([100]) toegang zou zijn tot de inhoud van elektronische communicatie.

3.1.2. Doeltreffende rechtsbescherming

(91) De Commissie heeft een beoordeling uitgevoerd van zowel de toezichtsmechanismen die in de Verenigde Staten bestaan met betrekking tot inmengingen van Amerikaanse inlichtingendiensten in naar de Verenigde Staten doorgegeven persoonsgegevens, als de individuele verhaalsmogelijkheden die betrokkenen uit de EU ter beschikking staan.

Toezicht

(92) De Amerikaanse inlichtingendiensten zijn onderworpen aan diverse controle- en toezichtsmechanismen die onder de drie machten van de Staat vallen. Het gaat daarbij om interne en externe instanties binnen de uitvoerende macht, een aantal Committees (commissies) van het Congres, alsook gerechtelijk toezicht; dat laatste toezicht betreft specifiek activiteiten op grond van de FISA.

(93) Ten eerste zijn de inlichtingenactiviteiten van Amerikaanse autoriteiten onderworpen aan uitgebreid toezicht binnen de uitvoerende macht.

(94) Volgens sectie 4(a)(iv) van PPD-28 omvatten de beleidslijnen en procedures van de onderdelen van de inlichtingendiensten „passende maatregelen om het toezicht op de toepassing van de waarborgen ter bescherming van persoonsgegevens te vergemakkelijken"; deze maatregelen moeten periodieke audits omvatten ([101]).

([98]) Zie arrest Schrems, punt 91, met verdere verwijzingen.
([99]) Arrest Schrems, punt 93.
([100]) Zie arrest Schrems, punt 94.
([101]) ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28 (De bescherming van ieders persoonsgegevens: verslag over de stand van zaken van de ontwikkeling en uitvoering van procedures krachtens PPD-28), blz. 7. Zie bv. CIA, Signals Intelligence Activities (Activiteiten met betrekking tot inlichtingen uit berichtenverkeer), blz. 6 (Compliance)(Naleving); FBI, Presidential Policy Directive 28 Policies and Procedures (Beleid en procedures op grond van PPD-28), sectie III (A)(4), (B)(4); NSA, PPD-28 Section 4 Procedures (Procedures op grond van sectie 4 van PPD-28), 12 januari 2015, sectie 8.1, 8.6(c).

(95) Er zijn in dit verband meerdere lagen van toezicht tot stand gebracht, waaronder de functionarissen voor de burgerlijke vrijheden en de privacy, de Inspectors General, het Civil Liberties and Privacy Office van het ODNI, de Privacy and Civil Liberties Oversight Board en de President's Intelligence Oversight Board. Deze toezichtfuncties worden ondersteund door gespecialiseerd personeel in alle diensten ([102]).

(96) Zoals toegelicht door de Amerikaanse overheid ([103]) zijn er *functionarissen voor de burgerlijke vrijheden en de privacy* met toezichtsverantwoordelijkheden binnen de verschillende ministeries met verantwoordelijkheden op het gebied van inlichtingen en inlichtingendiensten ([104]). 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/dienst 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 ODNI ([105])). Het hoofd van het ministerie/de dienst moet er op zijn beurt voor zorgen dat de functionaris alle informatie krijgt en toegang krijgt tot al het materiaal dat nodig is om zijn taken uit te voeren. De functionarissen voor de burgerlijke vrijheden en de privacy brengen periodiek verslag uit aan het Congres en de Privacy and Civil Liberties Oversight Board, onder meer over het aantal en de aard van de klachten die het ministerie/de dienst 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 ([106]). Volgens de beoordeling door de nationale gegevensbeschermingsautoriteiten kan het interne toezicht dat door de functionarissen voor de burgerlijke vrijheden en de privacy wordt uitgeoefend, als „redelijk solide" worden beschouwd, ook al zijn die functionarissen volgens hen niet onafhankelijk genoeg ([107]).

(97) Bovendien heeft elk onderdeel van de inlichtingendiensten een eigen *Inspector General*, die onder andere belast is met het toezicht op buitenlandse inlichtingenactiviteiten ([108]). Binnen het ODNI is dat het Office of the Inspector General (bureau van de Inspector General), 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 ([109]). De Inspectors General zijn statutair onafhankelijke ([110]) eenheden die verantwoordelijk zijn 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 ([111]). Zij zijn gemachtigd om toegang te hebben tot alle gegevens, verslagen, audits, controles, documenten,

([102]) Bij de NSA werken bijvoorbeeld meer dan 300 gespecialiseerde personeelsleden bij het Directorate for Compliance. Zie de verklaringen van het ODNI (bijlage VI), blz. 7.

([103]) Zie het mechanisme van de ombudsman (bijlage III), sectie 6(b) (i) tot (iii).

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

([105]) Als het Civil Liberties and Privacy Office van het ODNI een klacht ontvangt, zal dit volgens de Amerikaanse overheid ook met andere onderdelen van de inlichtingendiensten afstemmen hoe die klacht verder moet te worden verwerkt binnen de inlichtingendiensten. Zie het mechanisme van de ombudsman (bijlage III), sectie 6(b) (ii).

([106]) Zie 42 U.S.C. § 2000ee-1 (f)(1),(2).

([107]) Advies 01/2016 van de Artikel 29-werkgroep gegevensbescherming inzake het ontwerpbesluit over de adequaatheid van het Europees-Amerikaanse privacyschild (aangenomen op 13 april 2016), blz. 41.

([108]) Verklaringen van het ODNI (bijlage VI), blz. 7. Zie bv. NSA, PPD-28 Section 4 Procedures (Procedures op grond van sectie 4 van PPD-28), 12 januari 2015, sectie 8.1; CIA, Signals Intelligence Activities (Activiteiten met betrekking tot inlichtingen uit berichtenverkeer), blz. 7 (Responsibilities) (Verantwoordelijkheden).

([109]) Deze Inspector General (die in oktober 2010 is benoemd) is benoemd door de president, met bevestiging van de Senaat, en kan alleen door de president worden ontslagen, niet door de Director of National Intelligence.

([110]) Deze Inspectors General 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 Inspector General 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 (Inspector General van het ministerie van Justitie); § 8E (Inspector General van het ministerie van Justitie), § 8G (d)(2)(A),(B) (Inspector General van de NSA); 50. U.S.C. § 403q (b) (Inspector General van de CIA); Intelligence Authorization Act For Fiscal Year 2010, sectie 405(f) (Inspector General voor de inlichtingendiensten). Volgens de beoordeling van de nationale gegevensbeschermingsautoriteiten voldoen de Inspectors General waarschijnlijk aan het criterium van organisatorische onafhankelijkheid zoals dat door het Hof van Justitie en het Europees Hof voor de rechten van de mens is omschreven, ten minste vanaf het ogenblik waarop de nieuwe benoemingsprocedure op allen van toepassing is. Zie advies 01/2016 van de Artikel 29-werkgroep gegevensbescherming inzake het ontwerpbesluit over de adequaatheid van het Europees-Amerikaanse privacyschild (aangenomen op 13 april 2016), blz. 40.

([111]) Zie de verklaringen van het ODNI (bijlage VI), blz. 7. Zie ook de Inspector General Act of 1978, zoals gewijzigd, Pub. L. 113-126 van 7 juli 2014.

papieren, aanbevelingen en ander relevant materiaal, zo nodig door een dwangbevel, en kunnen getuigenverklaringen afnemen ([112]). Hoewel de Inspectors General alleen niet-bindende aanbevelingen voor corrigerende maatregelen kunnen doen, worden hun verslagen, met inbegrip van de vervolgmaatregelen (of het ontbreken daarvan) openbaar gemaakt en bovendien aan het Congres toegezonden, dat op basis daarvan zijn toezichtsfunctie kan uitoefenen ([113]).

(98) Bovendien is de *Privacy and Civil Liberties Oversight Board*, een onafhankelijke instantie ([114]) binnen de uitvoerende macht die bestaat uit een raad van vijf leden uit beide politieke partijen ([115]) die door de president voor een vaste ambtstermijn van zes jaar zijn benoemd met goedkeuring van de Senaat, belast met taken op het gebied van het beleid inzake 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. Zij ontvangt de verslagen van de functionarissen voor de burgerlijke vrijheden en de privacy van verschillende federale ministeries/diensten ([116]), kan hun aanbevelingen doen en brengt regelmatig verslag uit aan de Committees van het Congres en de president ([117]). De Privacy and Civil Liberties Oversight Board moet ook, binnen de grenzen van zijn mandaat, een verslag voorbereiden waarin de tenuitvoerlegging van PPD-28 wordt beoordeeld.

(99) Ten slotte worden de bovengenoemde toezichtsmechanismen aangevuld door de binnen de President's Intelligence Advisory Board ingestelde *Intelligence Oversight Board*, die toezicht houdt op de naleving van de grondwet en alle geldende regels door de Amerikaanse inlichtingendiensten.

(100) Om het toezicht te vergemakkelijken, worden de onderdelen van de inlichtingendiensten aangemoedigd om informatiesystemen te ontwerpen die het mogelijk maken om de verzoeken of andere zoekopdrachten betreffende persoonsgegevens te bewaken, te registreren en te evalueren ([118]). De toezichthoudende en conformiteitsbeoordelingsinstanties zullen periodiek nagaan of de praktijken van de onderdelen van de inlichtingendiensten de persoonsgegevens in inlichtingen uit berichtenverkeer beschermen en of zij die procedures naleven ([119]).

(101) Deze toezichtsfuncties worden bovendien ondersteund door uitgebreide rapportagevereisten met betrekking tot niet-naleving. In het bijzonder moeten de procedures van de diensten waarborgen dat in geval van een belangrijk nalevingsprobleem betreffende persoonsgegevens van welke persoon dan ook, ongeacht nationaliteit, die uit inlichtingen uit berichtenverkeer zijn verzameld, dit probleem onmiddellijk wordt gemeld aan het hoofd van het betrokken onderdeel van de inlichtingendiensten, die op zijn beurt de Director of National Intelligence in kennis stelt, die krachtens PPD-28 zal bepalen of er corrigerende maatregelen noodzakelijk zijn ([120]). Bovendien moeten alle onderdelen van de inlichtingendiensten overeenkomstig E.O. 12333 verslag uitbrengen aan de Intelligence Oversight Board over gevallen van niet-naleving ([121]). Deze mechanismen zorgen ervoor dat het probleem op het

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

([113]) Zie de verklaringen van het ODNI (bijlage VI), blz. 7. Zie ook de Inspector General Act van 1978, §§ 4(5), 5. Volgens sectie 405(b)(3),(4) van de Intelligence Authorization Act For Fiscal Year 2010, Pub. L. 111-259 van 7 oktober 2010, zal de Inspector General van de inlichtingendiensten zowel de Director of National Intelligence als het Congres op de hoogte houden van de noodzaak, en de voortgang, van corrigerende maatregelen.

([114]) Volgens de beoordeling door de nationale gegevensbeschermingsautoriteiten heeft de Privacy and Civil Liberties Oversight Board in het verleden „laten zien dat hij onafhankelijke bevoegdheden heeft". Zie Advies 01/2016 van de Artikel 29-werkgroep gegevensbescherming inzake het ontwerpbesluit over de adequaatheid van het Europees-Amerikaanse privacyschild (aangenomen op 13 april 2016), blz. 42.

([115]) Daarnaast werken er bij de Privacy and Civil Liberties Oversight Board ongeveer twintig vaste personeelsleden. Zie https://www.pclob.gov/about-us/staff.html

([116]) 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.

([117]) Zie 42 U.S.C. § 2000ee. Zie ook het mechanisme van de ombudsman (bijlage III), sectie 6(b) (iv). De Privacy and Civil Liberties Oversight Board moet verslag uitbrengen wanneer een dienst van de uitvoerende macht weigert zijn advies te volgen.

([118]) ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28 (De bescherming van ieders persoonsgegevens: verslag over de stand van zaken van de ontwikkeling en uitvoering van procedures krachtens PPD-28), blz. 7.

([119]) Id. op blz. 8. Zie ook de verklaringen van het ODNI (bijlage VI), blz. 9.

([120]) ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28 (De bescherming van ieders persoonsgegevens: verslag over de stand van zaken van de ontwikkeling en uitvoering van procedures krachtens PPD-28), blz. 7. Zie bv. NSA, PPD-28 Section 4 Procedures (Procedures op grond van sectie 4 van PPD-28), 12 januari 2015, sectie 7.3, 8.7(c),(d); FBI, Presidential Policy Directive 28 Policies and Procedures (Beleid en procedures op grond van PPD-28), sectie III.(A)(4), (B)(4); CIA, Signals Intelligence Activities (Activiteiten met betrekking tot inlichtingen uit berichtenverkeer), blz. 6 (Compliance) (Naleving) en blz. 8 (Responsibilities) (Verantwoordelijkheden).

([121]) Zie E.O. 12333, sectie 1.6(c).

hoogste niveau van de inlichtingendiensten zal worden aangepakt. Als het om een niet-Amerikaan gaat, bepaalt de Director of National Intelligence, in overleg met de minister van Buitenlandse Zaken en het hoofd van het/de kennisgevende ministerie/dienst, of er stappen moeten worden ondernomen om de betrokken buitenlandse overheid op de hoogte te stellen, in overeenstemming met de bescherming van bronnen en methoden en van Amerikaans personeel ([122]).

(102) Ten tweede heeft het Amerikaanse Congres, met name de *House and Senate 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, met inbegrip van inlichtingen uit berichtenverkeer van de Verenigde Staten. Volgens de National Security Act zorgt de president ervoor „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" ([123]). Ook 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" ([124]). De leden van deze Committees hebben toegang tot gerubriceerde informatie en inlichtingenmethoden en -programma's ([125]).

(103) De rapportagevereisten zijn door latere wetten uitgebreid en verfijnd, zowel met betrekking tot de onderdelen van de inlichtingendiensten, de betrokken Inspectors General en de Attorney General. Zo schrijft de FISA voor dat de Attorney General de Senate and House Intelligence and Judiciary Committees „ten volle moet informeren" over de activiteiten van de overheid in het kader van bepaalde secties van de FISA ([126]). De FISA schrijft ook voor dat de overheid de Committees van het Congres moet voorzien van „afschriften van alle beslissingen, bevelen of adviezen van de Foreign Intelligence Surveillance Court of de Foreign Intelligence Surveillance Court of Review die een essentiële uitlegging of interpretatie bevatten" van bepalingen van de FISA. Met betrekking tot surveillance op grond van sectie 702 van de FISA wordt het toezicht met name 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 Attorney General waarin de toepassing van sectie 702 van de 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 ([127]), en een afzonderlijke halfjaarlijkse beoordeling van de Attorney General en de Director of National Intelligence waarin de naleving van de procedures om het doelwit te specificeren en de minimaliseringsprocedures wordt gedocumenteerd, inclusief de naleving van de procedures om te garanderen dat het verzamelen een geldig doel op het gebied van buitenlandse inlichtingen dient ([128]). Het Congres ontvangt tevens verslagen van de Inspectors General die bevoegd zijn om de naleving van de procedures om het doelwit te specificeren, de minimaliseringsprocedures en de richtsnoeren van de minister van Justitie door de diensten te evalueren.

(104) Overeenkomstig de USA Freedom Act van 2015 moet de Amerikaanse overheid elk jaar aan het Congres (en het publiek) onder andere het aantal gevraagde en ontvangen FISA-bevelen en -richtlijnen bekendmaken, evenals ramingen van het aantal Amerikanen en niet-Amerikanen die het doelwit van surveillance zijn ([129]). 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

([122]) PPD-28, sectie 4(a)(iv).
([123]) Zie sectie 501(a)(1) (50 U.S.C. § 413(a)(1)). Deze bepaling bevat de algemene vereisten met betrekking tot het toezicht van het Congres op het gebied van de nationale veiligheid.
([124]) Zie sectie 501(b) (50 U.S.C. § 413(b)).
([125]) Zie sectie 501(d) (50 U.S.C. § 413(d)).
([126]) Zie 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.
([127]) Zie 50 U.S.C. § 1881f.
([128]) Zie 50 U.S.C. § 1881a(l)(1).
([129]) Zie de USA Freedom Act van 2015, Pub. L. nr. 114-23, sectie 602(a). Bovendien voert de Director of National Intelligence overeenkomstig sectie 402 „in overleg met de Attorney General 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".

certificeringen, alsook van verzoeken op basis van national security letters, tegelijkertijd de mogelijkheid om onder bepaalde voorwaarden transparantieverslagen op te stellen) ([130]).

(105) Ten derde laten de inlichtingenactiviteiten van de Amerikaanse overheidsdiensten op basis van de FISA ruimte voor toetsing, en in sommige gevallen is voor de maatregelen voorafgaande toestemming vereist van de *Foreign Intelligence Surveillance Court (FISC)* ([131]), een onafhankelijke rechterlijke instantie ([132]), waarvan de beslissingen kunnen worden aangevochten voor de Foreign Intelligence Court of Review (FISCR) ([133]) en, uiteindelijk, de Supreme Court van de Verenigde Staten ([134]). In geval van voorafgaande toestemming moeten de verzoekende instanties (FBI, NSA, CIA enz.) een ontwerpverzoek indienen bij de juristen van het departement Nationale Veiligheid van het ministerie van Justitie, die het verzoek zullen onderzoeken en, indien nodig, om aanvullende informatie zullen vragen ([135]). Zodra het verzoek is afgerond, moet het worden goedgekeurd door de Attorney General, de Deputy Attorney General of de Assistant Attorney General for National Security ([136]). Vervolgens zal het ministerie van Justitie het verzoek indienen bij de FISC, die het verzoek zal beoordelen en een voorlopige beslissing zal nemen over de te volgen procedure ([137]). Als er een hoorzitting plaatsvindt, heeft de FISC de bevoegdheid om getuigenverklaringen af te nemen, die deskundig advies kunnen omvatten ([138]).

(106) De FISC (en de FISCR) worden ondersteund door een permanent panel van vijf personen die beschikken over deskundigheid op het gebied van nationale veiligheid en de burgerlijke vrijheden ([139]). 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 ([140]). 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 ([141]).

([130]) USA Freedom Act, sectie 602(a), 603(a).

([131]) Voor bepaalde soorten surveillance kan het echter een Amerikaanse magistrate judge zijn — die openbaar door de Chief Justice van de Verenigde Staten is aangewezen — die bevoegd is om verzoeken te behandelen en bevelen uit te vaardigen.

([132]) De FISC bestaat uit elf 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 komen. Zie sectie 103 FISA (50 U.S.C. 1803 (a)); Privacy and Civil Liberties Oversight Board, Sec. 215 Report (Verslag over sectie 215), blz. 174-187. 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 Privacy and Civil Liberties Oversight Board, Sec. 215 Report (Verslag over sectie 215), blz. 178; brief van de Honourable Reggie B. Walton, Presiding Judge, 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. 2-3.

([133]) De FISCR bestaat uit drie 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 sectie 103 FISA (50 U.S.C. § 1803 (b)).

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

([135]) Bijvoorbeeld aanvullende feitelijke details over het doelwit van de surveillance, technische informatie over de surveillancemethode of garanties met betrekking tot de manier waarop de verkregen informatie zal worden gebruikt en verspreid. Zie Privacy and Civil Liberties Oversight Board, Sec. 215 Report (Verslag over sectie 215), blz. 177.

([136]) 50 U.S.C. §§ 1804 (a), 1801 (g).

([137]) De FISC kan het verzoek goedkeuren, om nadere informatie verzoeken, vaststellen dat er een hoorzitting moet plaatsvinden of wijzen op een mogelijke afwijzing van het verzoek. Op basis van die voorlopige beslissing zal de overheid haar definitieve verzoek indienen. Daarbij kan het oorspronkelijke verzoek aanzienlijk worden gewijzigd op basis van de voorlopige opmerkingen van de rechter. Een groot percentage van de definitieve verzoeken wordt door de FISC goedgekeurd, maar een aanzienlijk deel daarvan is materieel gewijzigd ten opzichte van het oorspronkelijke verzoek, bv. 24 % van de verzoeken die in de periode juli-september 2013 werden goedgekeurd. Zie Privacy and Civil Liberties Oversight Board, Sec. 215 Report (Verslag over sectie 215), blz. 179; Walton-brief, blz. 3.

([138]) Privacy and Civil Liberties Oversight Board, Sec. 215 Report (Verslag over sectie 215), blz. 179, nr. 619.

([139]) 50 U.S.C. § 1803 (i)(1),(3)(A). Bij deze nieuwe wetgeving is gevolg gegeven aan de aanbevelingen van de Privacy and Civil Liberties Oversight Board om een groep deskundigen op het gebied van privacy en burgerlijke vrijheden te vormen die als *amicus curiae* kunnen optreden, zodat de FISC over juridische argumenten kan beschikken ter bevordering van de privacy en de burgerlijke vrijheden. Zie Privacy and Civil Liberties Oversight Board, Sec. 215 Report (Verslag over sectie 215), blz. 183-187.

([140]) 50 U.S.C. § 1803 (i)(2)(A). Volgens informatie van het ODNI hebben er al dergelijke benoemingen plaatsgevonden. Zie Signals Intelligence Reform (Hervorming van de inlichtingen uit berichtenverkeer), voortgangsverslag 2016.

([141]) 50 U.S.C. § 1803 (i)(2)(B).

(107) Met betrekking tot de twee wettelijke machtigingen voor surveillance in de FISA die het belangrijkst zijn voor doorgiften van gegevens in het kader van het EU-VS-privacyschild, verschilt het toezicht van de FISC.

(108) Op grond van sectie 501 van de FISA ([142]), die het verzamelen van „tastbare zaken (waaronder boeken, dossiers, papieren, documenten en andere zaken)" toestaat, moet het verzoek aan de FISC een uiteenzetting bevatten van de feiten waaruit blijkt dat er redelijke gronden zijn om aan te nemen dat de gezochte tastbare zaken relevant zijn voor een toegestaan onderzoek (anders dan een dreigingsevaluatie) dat wordt uitgevoerd om buitenlandse inlichtingen te verkrijgen die geen Amerikaan betreffen, of ter bescherming tegen internationaal terrorisme of heimelijke inlichtingenactiviteiten. Daarnaast moet het verzoek een opsomming bevatten van de door de Attorney General goedgekeurde minimaliseringsprocedures voor de bewaring en verspreiding van de verzamelde inlichtingen ([143]).

(109) Op grond van sectie 702 van de FISA ([144]) geeft de FISC daarentegen geen toestemming voor individuele surveillancemaatregelen; de FISC geeft in plaats daarvan toestemming voor surveillanceprogramma's (zoals PRISM en UPSTREAM) op basis van jaarlijkse certificeringen die door de Attorney General en de Director of National Intelligence worden voorbereid. Sectie 702 van de FISA maakt het mogelijk 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 ([145]). Het specificeren van doelwitten wordt door de NSA in twee stappen uitgevoerd. 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. Nadat die individuele personen zijn bepaald en na het doorlopen van een uitgebreid evaluatiemechanisme binnen de NSA als doelwit zijn goedgekeurd ([146]), 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) ([147]). Zoals aangegeven, bevatten de door de FISC goed te keuren certificeringen geen informatie over de individuele personen die het doelwit moeten worden, maar bepalen ze in plaats daarvan categorieën buitenlandse inlichtingen ([148]). De FISC beoordeelt niet — op grond van een redelijk vermoeden of een andere norm — of natuurlijke personen het juiste doelwit zijn om buitenlandse inlichtingen te verwerven ([149]), maar controleert de voorwaarde dat „het verkrijgen van buitenlandse inlichtingen een significant doel van de verwerving is" ([150]). Op grond van sectie 702 van de FISA mag de NSA immers alleen communicatie van niet-Amerikanen buiten de Verenigde Staten verzamelen als redelijkerwijs kan worden aangenomen dat een bepaald communicatiemiddel wordt gebruikt voor de doorgifte van buitenlandse inlichtingen (bv. in verband met internationaal terrorisme, nucleaire proliferatie of vijandige cyberactiviteiten). De besluiten dienaangaande zijn onderworpen aan gerechtelijke controle ([151]). Certificeringen moeten tevens voorzien in procedures om het doelwit te specificeren en minimaliseringsprocedures ([152]). De Attorney General en de

([142]) 50 U.S.C. § 1861.
([143]) 50 U.S.C. § 1861 (b).
([144]) 50 U.S.C. § 1881.
([145]) 50 U.S.C. § 1881a (a).
([146]) Zie Privacy and Civil Liberties Oversight Board, Sec. 702 Report (Verslag over sectie 702), blz. 46.
([147]) 50 U.S.C. § 1881a (h).
([148]) 50 U.S.C. § 1881a (g). Volgens de Privacy and Civil Liberties Oversight Board hadden deze categorieën tot dusver vooral betrekking op internationaal terrorisme en onderwerpen zoals de verwerving van massavernietigingswapens. Zie Privacy and Civil Liberties Oversight Board, Sec. 702 Report (Verslag over sectie 702), blz. 25.
([149]) Privacy and Civil Liberties Oversight Board, Sec. 702 Report (Verslag over sectie 702), blz. 27.
([150]) 50 U.S.C. § 1881a.
([151]) „Liberty and Security in a Changing World" (Vrijheid en veiligheid in een veranderende wereld), verslag en aanbevelingen van de President's Review Group on Intelligence and Communications Technologies, 12 december 2013, blz. 152.
([152]) 50 U.S.C.1881a (i).

Director of National Intelligence controleren de naleving en de diensten zijn verplicht eventuele gevallen van niet-naleving te melden aan de FISC ([153]) (en aan het Congres en de President's Intelligence Oversight Board), die op basis daarvan de toestemming kan wijzigen ([154]).

(110) Om het toezicht van de FISC efficiënter te maken, heeft de Amerikaanse overheid voorts toegezegd uitvoering te geven aan een aanbeveling van de Privacy and Civil Liberties Oversight Board om de FISC documentatie inzake besluiten over de specificatie van doelwitten op grond van sectie 702 te verstrekken, inclusief een aselecte steekproef van taakbladen, zodat de FISC kan beoordelen hoe in de praktijk aan de eis wordt voldaan dat het buitenlandse inlichtingenwerk gericht wordt uitgevoerd ([155]). Tegelijkertijd heeft de Amerikaanse overheid erkend dat de NSA-procedures om doelwitten te specificeren moeten worden herzien en hiertoe maatregelen genomen, teneinde de met buitenlands inlichtingenwerk verband houdende redenen voor besluiten over de specificatie van doelwitten beter te documenteren ([156]).

Individuele verhaalsmogelijkheden

(111) Op grond van het Amerikaanse recht staat betrokkenen uit de EU een aantal mogelijkheden ter beschikking als zij zich afvragen of hun persoonsgegevens zijn verwerkt (verzameld, geraadpleegd enz.) door onderdelen van de Amerikaanse inlichtingendiensten en, indien dat het geval is, of de in het Amerikaanse recht geldende beperkingen in acht zijn genomen. Deze mogelijkheden hebben voornamelijk betrekking op drie situaties: inmenging op grond van de FISA, onrechtmatige, opzettelijke toegang tot persoonsgegevens door overheidsfunctionarissen, en toegang tot informatie op grond van de Freedom of Information Act ([157]).

(112) Ten eerste voorziet de FISA in een aantal rechtsmiddelen, die ook openstaan voor niet-Amerikanen, om onrechtmatige elektronische surveillance aan te vechten ([158]). Natuurlijke personen kunnen onder meer langs civielrechtelijke weg een geldelijke schadevergoeding van de Verenigde Staten vorderen wanneer hen betreffende informatie onrechtmatig en opzettelijk is gebruikt of bekendgemaakt ([159]), voor de rechter een geldelijke schadevergoeding van Amerikaanse overheidsfunctionarissen in hun persoonlijke hoedanigheid („under colour of law"/onder het voorwendsel van het recht) vorderen ([160]), en de wettigheid van de surveillance aanvechten (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 ([161]).

(113) Ten tweede heeft de Amerikaanse overheid de Commissie gewezen op een aantal aanvullende mogelijkheden voor betrokkenen uit de EU om gerechtelijke stappen te ondernemen tegen overheidsfunctionarissen vanwege onrechtmatige toegang van de overheid tot of gebruik door de overheid van persoonsgegevens, onder meer voor

([153]) Overeenkomstig regel 13(b) van het reglement van orde van de FISC moet de overheid de Court onmiddellijk schriftelijk in kennis stellen wanneer aan het licht komt dat een door de Court verleende toestemming of goedkeuring is toegepast op een wijze die niet in overeenstemming is met de toestemming of goedkeuring van de Court, of met het toepasselijke recht. Die regel schrijft tevens voor dat de overheid de Court schriftelijk in kennis moet stellen van de feiten en omstandigheden die van belang zijn voor deze niet-naleving. Doorgaans zal de overheid een definitieve kennisgeving op grond van regel 13(b) indienen zodra de relevante feiten bekend zijn en eventuele ongeoorloofd verzamelde gegevens zijn vernietigd. Zie de Walton-brief, blz. 10.

([154]) 50 U.S.C. § 1881 (l). Zie ook Privacy and Civil Liberties Oversight Board, Sec. 702 Report (Verslag over sectie 702), blz. 66-76; 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. Het verzamelen van persoonsgegevens voor inlichtingenwerk op grond van sectie 702 van de FISA is aan intern en extern toezicht onderworpen binnen de uitvoerende macht. Het interne toezicht omvat onder andere interne nalevingsprogramma's om de naleving van de procedures om het doelwit te specificeren en de minimaliseringsprocedures te beoordelen en te controleren, de rapportage van gevallen van niet-naleving, zowel intern als extern aan het ODNI, het ministerie van Justitie, het Congres en de FISC, en jaarlijkse evaluaties die aan dezelfde instanties worden toegezonden. Het externe toezicht bestaat voornamelijk uit beoordelingen van de specificatie van doelwitten en de minimalisering door het ODNI, het ministerie van Justitie en de Inspectors General, die op hun beurt verslag uitbrengen aan het Congres en de FISC, onder meer over gevallen van niet-naleving. Belangrijke gevallen van niet-naleving moeten onmiddellijk aan de FISC worden gemeld en aan de andere instanties in een kwartaalverslag. Zie Privacy and Civil Liberties Oversight Board, Sec. 702 Report (Verslag over sectie 702), blz. 66-77.

([155]) Privacy and Civil Liberties Oversight Board, Recommendations Assessment Report (Evaluatieverslag over de uitvoering van de aanbevelingen), 29 januari 2015, blz. 20.

([156]) Privacy and Civil Liberties Oversight Board, Recommendations Assessment Report (Evaluatieverslag over de uitvoering van de aanbevelingen), 29 januari 2015, blz. 16.

([157]) Daarnaast bepaalt sectie 10 van de Classified Information Procedures Act dat de Verenigde Staten bij elke vervolging waarin moet worden aangetoond dat materiaal gerubriceerde informatie vormt (bv. omdat het om redenen van nationale veiligheid moet worden beschermd tegen niet-toegestane openbaarmaking), de verweerder in kennis moeten stellen van de gedeelten van het materiaal waarop zij naar verwachting redelijkerwijs een beroep zullen doen om het aspect gerubriceerde informatie van de overtreding aan te tonen.

([158]) Zie voor het volgende de verklaringen van het ODNI (bijlage VI), blz. 16.

([159]) 18 U.S.C. § 2712.

([160]) 50 U.S.C. § 1810.

([161]) 50 U.S.C. § 1806.

vermeende doeleinden van nationale veiligheid (te weten de Computer Fraud Abuse Act ([162]), de Electronic Communications Privacy Act ([163]) en de Right to Financial Privacy Act ([164])). Al deze gronden voor vorderingen 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) ([165]). Een meer algemene verhaalsmogelijkheid wordt geboden door de Administrative Procedure Act (5 U.S.C. § 702), 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. 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" ([166]).

(114) Ten slotte heeft de Amerikaanse overheid gewezen op de Freedom of Information Act als middel voor niet-Amerikanen om toegang te krijgen tot bestaande informatiebestanden van federale diensten, onder meer wanneer die de persoonsgegevens van de natuurlijke persoon bevatten ([167]). Gezien haar toepassingsgebied voorziet de Freedom of Information Act niet in een individuele verhaalsmogelijkheid tegen inmenging in persoonsgegevens als zodanig, al zou zij natuurlijke personen in beginsel in staat kunnen stellen om toegang te krijgen tot relevante informatie waarover de nationale inlichtingendiensten beschikken. Zelfs in dit opzicht lijken de mogelijkheden beperkt te zijn, aangezien diensten informatie mogen achterhouden die onder bepaalde opgesomde uitzonderingen valt, waaronder toegang tot gerubriceerde informatie over de nationale veiligheid en informatie over rechtshandhavingsonderzoeken ([168]). Het gebruik van dergelijke uitzonderingen door de nationale inlichtingendiensten kan echter worden aangevochten door natuurlijke personen, die zowel administratief als gerechtelijk beroep kunnen instellen.

(115) Hoewel natuurlijke personen, waaronder betrokkenen uit de EU, over een aantal verhaalsmogelijkheden beschikken wanneer zij aan onrechtmatige (elektronische) surveillance om doeleinden van nationale veiligheid zijn onderworpen, is het evengoed duidelijk dat ten minste enkele rechtsgrondslagen waarop de Amerikaanse inlichtingendiensten zich kunnen baseren (bv. E.O. 12333), niet worden bestreken. Bovendien bestaan er weliswaar in beginsel gerechtelijke verhaalsmogelijkheden voor niet-Amerikanen, zoals voor surveillance op grond van de FISA, maar de mogelijke gronden zijn beperkt ([169]) en vorderingen van natuurlijke personen (waaronder Amerikanen) zullen niet-ontvankelijk worden verklaard wanneer zij geen „status" kunnen aantonen ([170]), waardoor de toegang tot gewone rechterlijke instanties wordt beperkt ([171]).

(116) Om te voorzien in een aanvullend verhaalsmechanisme dat openstaat voor alle betrokkenen uit de EU, heeft de Amerikaanse overheid besloten een nieuw ombudsmanmechanisme in het leven te roepen, zoals uiteengezet in de brief van de Amerikaanse minister van Buitenlandse Zaken aan de Commissie, die is opgenomen in bijlage III bij dit besluit. Dit mechanisme heeft als basis de aanstelling krachtens PPD-28 van een hoofdcoördinator (op het niveau van de onderminister) binnen het ministerie van Buitenlandse Zaken als contactpunt voor buitenlandse overheden om hun bezorgdheid te uiten met betrekking tot Amerikaanse activiteiten met betrekking tot inlichtingen uit berichtenverkeer, maar gaat aanzienlijk verder dan dit oorspronkelijke concept.

([162]) 18 U.S.C. § 1030.
([163]) 18 U.S.C. §§ 2701-2712.
([164]) 12 U.S.C. § 3417.
([165]) Verklaringen van het ODNI (bijlage VI), blz. 17.
([166]) 5 U.S.C. § 706(2)(A).
([167]) 5 U.S.C. § 552. Soortgelijke wetten bestaan op het niveau van de staten.
([168]) 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).
([169]) Zie de verklaringen van het ODNI (bijlage VI), blz. 16. Volgens de verstrekte uitleg is voor de beschikbare gronden ofwel het bestaan van schade vereist (18 U.S.C. § 2712; 50 U.S.C. § 1810) ofwel een bewijs dat de overheid voornemens is uit elektronische surveillance van de betrokkene verkregen of afgeleide informatie tegen die persoon te gebruiken of bekend te maken in een gerechtelijke of administratieve procedure in de Verenigde Staten (50 U.S.C. § 1806). Zoals het Hof van Justitie herhaaldelijk heeft benadrukt is het voor de vaststelling van het bestaan van een ingreep in het grondrecht op privacy evenwel niet van belang of de betrokkene nadelige gevolgen heeft ondervonden van die ingreep. Zie arrest Schrems, punt 89, met verdere verwijzingen.
([170]) Dit ontvankelijkheidscriterium vloeit voort uit het vereiste van „case or controversy" in artikel III van de Amerikaanse grondwet.
([171]) Zie Clapper/Amnesty International USA, 133 S.Ct. 1138, 1144 (2013). Wat het gebruik van national security letters betreft, voorziet de USA Freedom Act (sectie 502(f)-503) erin dat verplichtingen inzake niet-openbaarmaking periodiek worden herzien en dat de ontvangers van national security letters op de hoogte worden gebracht wanneer de feiten niet langer een verplichting inzake niet-openbaarmaking rechtvaardigen (zie de verklaringen van het ODNI (bijlage VI), blz. 13). Hierdoor wordt echter niet gewaarborgd dat de betrokkene uit de EU ervan op de hoogte wordt gebracht dat hij of zij het doelwit van een onderzoek is geweest.

(117) Het ombudsmanmechanisme zal er met name volgens de toezeggingen van de Amerikaanse overheid voor zorgen dat individuele klachten naar behoren worden onderzocht en aangepakt, en dat natuurlijke personen een onafhankelijke bevestiging ontvangen dat de Amerikaanse wetten zijn nageleefd of, in geval van een schending van die wetten, dat de niet-naleving verholpen is ([172]). Het mechanisme omvat „de privacyschildombudsman", d.w.z. de onderminister en verder personeel alsook andere toezichtsinstanties die bevoegd zijn om toezicht te houden op de verschillende onderdelen van de inlichtingendiensten die met de privacyschildombudsman zullen moeten samenwerken om klachten te behandelen. Wanneer het verzoek van een natuurlijke persoon de verenigbaarheid van surveillance met de Amerikaanse wetgeving betreft, zal de privacyschildombudsman met name een beroep kunnen doen op onafhankelijke toezichtsinstanties met onderzoeksbevoegdheden (zoals de Inspectors General of de Privacy and Civil Liberties Oversight Board). In elke zaak zorgt de minister van Buitenlandse Zaken ervoor dat de ombudsman de middelen zal hebben om ervoor te zorgen dat zijn antwoord op individuele verzoeken gebaseerd is op alle nodige informatie.

(118) Door deze „samengestelde structuur" garandeert het ombudsmanmechanisme onafhankelijk toezicht en individueel verhaal. Bovendien garandeert de samenwerking met andere toezichtsinstanties toegang tot de nodige deskundigheid. Door ten slotte een verplichting in te voeren voor de privacyschildombudsman om de naleving te bevestigen of niet-naleving te verhelpen, is het mechanisme de uitdrukking van het engagement van de Amerikaanse overheid als geheel om klachten van natuurlijke personen uit de EU te behandelen en op te lossen.

(119) Ten eerste zal de privacyschildombudsman, anders dan een zuiver intergouvernementeel mechanisme, individuele klachten ontvangen en beantwoorden. Die klachten kunnen worden gericht aan de toezichthoudende autoriteiten van de lidstaten die bevoegd zijn voor het toezicht op de nationale veiligheidsdiensten en/of de verwerking van persoonsgegevens door overheidsinstanties, die de klachten zullen voorleggen aan een gecentraliseerde EU-instantie die ze naar de privacyschildombudsman zal doorsluizen ([173]). Dit zal in feite ten goede komen aan de natuurlijke personen uit de EU, omdat zij zich in hun eigen taal tot een nationale instantie „dicht bij huis" kunnen wenden. Het zal de taak zijn van die autoriteit om de natuurlijke persoon te ondersteunen bij het indienen van een verzoek aan de privacyschildombudsman dat alle basisinformatie bevat en dus als „volledig" kan worden beschouwd. De natuurlijke persoon hoeft niet aan te tonen dat zijn of haar persoonsgegevens inderdaad door de Amerikaanse overheid zijn geraadpleegd door middel van activiteiten met betrekking tot inlichtingen uit berichtenverkeer.

(120) Ten tweede zegt de Amerikaanse overheid toe ervoor te zorgen dat de privacyschildombudsman in de uitoefening van zijn functies een beroep zal kunnen doen op de samenwerking van andere mechanismen voor toezicht op en controle van de naleving die in de Amerikaanse wetgeving bestaan. Daarbij zal het soms gaan om nationale inlichtingenautoriteiten, met name wanneer het verzoek moet worden uitgelegd als een verzoek om toegang tot documenten op grond van de Freedom of Information Act. In andere gevallen, meer bepaald wanneer verzoeken betrekking hebben op de verenigbaarheid van surveillance met de Amerikaanse wetgeving, zal voor de samenwerking een beroep worden gedaan op onafhankelijke toezichtsinstanties (bv. de Inspectors General) die de verantwoordelijkheid en de bevoegdheid hebben om een grondig onderzoek te verrichten (met name door toegang tot alle relevante documenten en de bevoegdheid om informatie en verklaringen te vragen) en niet-naleving aan te pakken ([174]). De privacyschildombudsman zal ook kwesties ter beoordeling kunnen verwijzen naar de Privacy and Civil Liberties Oversight Board ([175]). Wanneer een van deze toezichtsinstanties niet-naleving heeft vastgesteld, zal het betrokken onderdeel van de inlichtingendiensten de niet-naleving moeten verhelpen, omdat alleen dan de ombudsman aan de natuurlijke persoon een „positief" antwoord zal kunnen geven (namelijk dat de niet-naleving is verholpen) waartoe de Amerikaanse overheid zich heeft verbonden. In het kader van de

([172]) Ingeval de klager toegang wenst tot documenten die in handen zijn van Amerikaanse overheidsdiensten, zijn de regels en procedures van de Freedom of Information Act van toepassing. Dit omvat de mogelijkheid gerechtelijke stappen te ondernemen (in plaats van onafhankelijk toezicht) ingeval het verzoek wordt afgewezen, onder de voorwaarden die in de Freedom of Information Act zijn vastgesteld.

([173]) Overeenkomstig het ombudsmanmechanisme (bijlage III), sectie 4(f), zal de privacyschildombudsman rechtstreekse contacten onderhouden met de EU-instantie voor de behandeling van individuele klachten, die op haar beurt verantwoordelijk zal zijn voor de communicatie met de natuurlijke persoon die het verzoek indient. Indien rechtstreekse communicatie deel uitmaakt van de „onderliggende processen" die de gevraagde oplossing kunnen bieden (bv. een verzoek om toegang op grond van de Freedom of Information Act, zie sectie 5), zal deze communicatie plaatsvinden volgens de toepasselijke procedures.

([174]) Zie het ombudsmanmechanisme (bijlage III), sectie 2(a). Zie ook de overwegingen 0-0.

([175]) Zie het ombudsmanmechanisme (bijlage III), sectie 2(c). Volgens de verklaringen van de Amerikaanse overheid evalueert de Privacy and Civil Liberties Oversight Board voortdurend de beleidslijnen en procedures, alsook de uitvoering daarvan, van de Amerikaanse autoriteiten die verantwoordelijk zijn voor terrorismebestrijding, om te bepalen of hun activiteiten „de privacy en burgerlijke vrijheden naar behoren beschermen en in overeenstemming zijn met de toepasselijke wet- en regelgeving en beleidsmaatregelen inzake de privacy en de burgerlijke vrijheden". Daarnaast is het zo dat de Privacy and Civil Liberties Oversight Board „verslagen en andere informatie van de functionarissen voor de burgerlijke vrijheden en de privacy ontvangt en beoordeelt en hun, in voorkomend geval, aanbevelingen doet met betrekking tot hun activiteiten".

samenwerking zal de privacyschildombudsman ook worden ingelicht over het resultaat van het onderzoek en zal hij de middelen hebben om ervoor te zorgen dat hij alle informatie ontvangt die hij nodig heeft om zijn antwoord voor te bereiden.

(121) Ten slotte zal de privacyschildombudsman onafhankelijk zijn van — en dus vrij zijn van instructies van — de Amerikaanse inlichtingendiensten ([176]). Dit is van groot belang, omdat de ombudsman zal moeten „bevestigen" i) dat de klacht naar behoren is onderzocht en ii) dat de desbetreffende Amerikaanse wetgeving — met inbegrip van met name de in bijlage VI opgenomen beperkingen en waarborgen — is nageleefd of, in het geval van niet-naleving, dat de schending verholpen is. Om die onafhankelijke bevestiging te kunnen geven, zal de privacyschildombudsman de nodige informatie met betrekking tot het onderzoek moeten ontvangen om te beoordelen of het antwoord aan de klager correct is. Daarnaast heeft de minister van Buitenlandse Zaken toegezegd dat hij ervoor zal zorgen dat de onderminister de functie van privacyschildombudsman objectief en vrij van onbehoorlijke beïnvloeding die een effect op het te geven antwoord kan hebben, zal uitoefenen.

(122) Globaal gezien garandeert dit mechanisme dat individuele klachten grondig zullen worden onderzocht en zullen worden opgelost, en dat daarbij ten minste op het gebied van surveillance onafhankelijke toezichtsinstanties met de nodige deskundigheid en onderzoeksbevoegdheden betrokken zullen zijn, alsook een ombudsman die zijn functies vrij van onbehoorlijke, met name politieke, invloed zal kunnen uitoefenen. Bovendien zullen natuurlijke personen een klacht kunnen indienen zonder dat zij hoeven aan te tonen, of zelfs maar een begin van bewijs te leveren, dat zij het voorwerp van surveillance zijn geweest ([177]). Gelet op deze kenmerken is de Commissie ervan overtuigd dat er passende en doeltreffende garanties tegen misbruik zijn.

(123) Op basis van al het bovenstaande concludeert de Commissie dat de Verenigde Staten zorgen voor doeltreffende rechtsbescherming tegen ingrepen door de Amerikaanse inlichtingendiensten in de grondrechten van de personen van wie de persoonsgegevens in het kader van het EU-VS-privacyschild uit de Unie naar de Verenigde Staten worden doorgegeven.

(124) In dit verband neemt de Commissie nota van het arrest van het Hof van Justitie in de zaak Schrems, waarin is bepaald dat „een regeling die niet in enige beroepsmogelijkheid voor de justitiabele voorziet om toegang tot de hem betreffende persoonsgegevens te verkrijgen, of rectificatie of verwijdering van die gegevens, de wezenlijke inhoud van het grondrecht op een effectieve voorziening in rechte zoals neergelegd in artikel 47 van het Handvest niet [eerbiedigt]" ([178]). Uit de beoordeling van de Commissie is gebleken dat die beroepsmogelijkheden in de Verenigde Staten voorhanden zijn, onder meer door de invoering van het ombudsmanmechanisme. Het ombudsmanmechanisme biedt onafhankelijk toezicht met onderzoeksbevoegdheden. In het kader van de voortdurende monitoring van het privacyschild door de Commissie, waaronder de jaarlijkse gezamenlijke evaluatie waarbij ook de ombudsman betrokken is, zal de doeltreffendheid van dit mechanisme opnieuw worden beoordeeld.

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

(125) Wat betreft de inmenging in het kader van het EU-VS-privacyschild doorgegeven persoonsgegevens ten behoeve van de rechtshandhaving, heeft de Amerikaanse overheid (via het ministerie van Justitie) zekerheid verstrekt over de toepasselijke beperkingen en waarborgen waarmee volgens de beoordeling van de Commissie een passend beschermingsniveau wordt aangetoond.

([176]) Zie arrest van het Europees Hof voor de rechten van de mens (grote kamer) van 4 december 2015, Zakharov/Rusland, verzoekschrift nr. 47143/06, punt 275, waarin het volgende is bepaald: „Hoewel het in beginsel wenselijk is om de toezichthoudende controle aan een rechter toe te vertrouwen, kan toezicht door niet-gerechtelijke instanties verenigbaar met het Verdrag worden geacht, mits de toezichthoudende instantie onafhankelijk is van de autoriteiten die de surveillance uitvoeren, en voldoende en doeltreffende toezichthoudende bevoegdheden heeft."

([177]) Zie arrest van 18 mei 2010, Kennedy/Verenigd Koninkrijk, verzoekschrift nr. 26839/05, punt 167.

([178]) Arrest Schrems, punt 95. Blijkens de punten 91 en 96 van het arrest heeft punt 95 betrekking op het niveau van bescherming dat binnen de rechtsorde van de Unie wordt gegarandeerd, en moet het niveau van bescherming in het derde land „in grote lijnen" daarmee overeenkomen. Volgens de punten 73 en 74 van het arrest vereist dit niet dat het niveau van bescherming of de middelen die het derde land kan inzetten, identiek moeten zijn, maar wel dat die middelen in de praktijk doeltreffend genoeg blijken te zijn.

(126) Volgens deze informatie is op grond van het vierde amendement van de Amerikaanse grondwet ([179]) voor huiszoekingen en inbeslagnemingen door rechtshandhavingsinstanties in beginsel ([180]) een rechterlijk bevel op grond van een „redelijk vermoeden" vereist. In de weinige specifiek vastgestelde en uitzonderlijke gevallen waarin geen bevel vereist is ([181]), is de rechtshandhaving onderworpen aan een „redelijkheidstoets" ([182]). Of een huiszoeking of inbeslagneming redelijk is, wordt „bepaald door enerzijds te beoordelen in welke mate die inbreuk maakt op de privacy van een persoon en anderzijds in welke mate die noodzakelijk is ter bevordering van rechtmatige overheidsbelangen" ([183]). Meer in het algemeen garandeert het vierde amendement privacy en waardigheid en beschermt het tegen willekeurig ingrijpen door overheidsfunctionarissen ([184]). Deze concepten weerspiegelen het idee van noodzaak en evenredigheid in het recht van de Unie. Zodra de rechtshandhavingsautoriteiten de in beslag genomen goederen niet langer als bewijs nodig hebben, moeten ze worden teruggegeven ([185]).

(127) Hoewel het recht van het vierde amendement zich niet uitstrekt tot niet-Amerikanen die niet in de Verenigde Staten wonen, profiteren deze laatsten toch indirect van de bescherming van dat artikel, omdat de persoonsgegevens in handen zijn van Amerikaanse ondernemingen, met tot gevolg dat de rechtshandhavingsautoriteiten in elk geval om een gerechtelijk bevel moeten vragen (of ten minste het vereiste van redelijkheid moeten eerbiedigen) ([186]). Verdere bescherming wordt geboden door bijzondere wetten, maar ook door de richtsnoeren van het ministerie van Justitie, waardoor de toegang tot gegevens ten behoeve van de rechtshandhaving wordt beperkt om redenen die met noodzakelijkheid en evenredigheid gelijkstaan (bv. door te vereisen dat de FBI de minst ingrijpende onderzoeksmethoden als haalbaar gebruikt, rekening houdend met de gevolgen voor de privacy en de burgerlijke vrijheden) ([187]). Volgens de verklaringen van de Amerikaanse overheid geldt dezelfde of grotere bescherming voor rechtshandhavingsonderzoeken op het niveau van de staten (met betrekking tot onderzoek dat krachtens de wetgeving van de staten wordt uitgevoerd) ([188]).

(128) Een voorafgaande gerechtelijke toestemming van een rechter of grand jury (een onderzoekskamer van de rechtbank die door een rechter of magistrate wordt samengesteld) is niet in alle zaken vereist ([189]), maar administratieve dwangbevelen zijn beperkt tot specifieke zaken en zullen aan onafhankelijke gerechtelijke controle worden onderworpen, tenminste als de overheid bij de rechter handhaving vordert ([190]).

([179]) Het vierde amendement bepaalt het volgende: „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." Slechts (magistrate) judges kunnen huiszoekingsbevelen afgeven. Federale bevelen voor het kopiëren van elektronisch opgeslagen informatie zijn voorts onderworpen aan rule 41 van de Federal Rules of Criminal Procedure.

([180]) De Supreme Court heeft herhaaldelijk verklaard dat huiszoekingen zonder bevel „uitzonderlijk" moeten zijn. Zie bv. Johnson/United States, 333 U.S. 10, 14 (1948); McDonald/United States, 335 U.S. 451, 453 (1948); Camara/Municipal Court, 387 U.S. 523, 528-29 (1967); G.M. Leasing Corp./United States, 429 U.S. 338, 352-53, 355 (1977). Daarnaast beklemtoont de Supreme Court regelmatig dat „de meest essentiële constitutionele regel op dit gebied is dat huiszoekingen die buiten de gerechtelijke procedure gebeuren, zonder voorafgaande goedkeuring door een rechter of magistraat, op grond van het vierde — amendement *in se* onredelijk zijn, behoudens enkele specifiek vastgestelde en duidelijk afgebakende uitzonderingen". Zie bv. Coolidge/New Hampshire, 403 U.S. 443, 454-55 (1971); G.M. Leasing Corp./United States, 429 U.S. 338, 352-53, 358 (1977).

([181]) City of Ontario/Quon, 130 S. Ct. 2619, 2630 (2010).

([182]) Zie Privacy and Civil Liberties Oversight Board, Sec. 215 Report (Verslag over sectie 215), blz. 107, waar wordt verwezen naar Maryland/King, 133 S. Ct. 1958, 1970 (2013).

([183]) Privacy and Civil Liberties Oversight Board, Sec. 215 Report (Verslag over sectie 215), blz. 107, waar wordt verwezen naar Samson/California, 547 U.S. 843, 848 (2006).

([184]) City of Ontario/Quon, 130 S. Ct. 2619, 2630 (2010), 2627.

([185]) Zie bv. United States/Wilson, 540 F.2d 1100 (D.C. Cir. 1976).

([186]) Zie arrest van het Europees Hof voor de rechten van de mens (grote kamer) van 4 december 2015, Zakharov/Rusland, verzoekschrift nr. 47143/06, punt 269, waarin het volgende is bepaald: „Het vereiste van een bevel tot onderschepping aan de provider van de communicatiediensten om toegang te krijgen tot het communicatieverkeer van een persoon, is een van de belangrijke waarborgen tegen misbruik door de rechtshandhavingsautoriteiten, waardoor in alle gevallen van onderschepping een behoorlijke toestemming wordt verkregen."

([187]) Verklaringen van het ministerie van Justitie van de Verenigde Staten (bijlage VII), blz. 4, met verdere verwijzingen.

([188]) Verklaringen van het ministerie van Justitie (bijlage VII), nr. 2.

([189]) Volgens de informatie die de Commissie heeft ontvangen, en los van specifieke gebieden die waarschijnlijk niet relevant zijn voor de doorgifte van gegevens in het kader van het EU-VS-privacyschild (bv. onderzoeken naar fraude in de gezondheidszorg, kindermisbruik of zaken betreffende gereguleerde stoffen), gaat het voornamelijk om bepaalde toestemmingen op grond van de Electronic Communications Privacy Act, te weten verzoeken om basisinformatie over abonnees, sessies en facturering (18 U.S.C. § 2703(c)(1), (2), bv. adres, soort/lengte van de dienst) en om de inhoud van e-mails die ouder zijn dan 180 dagen (18 U.S.C. § 2703(a), (b)). In het laatste geval moet de betrokkene echter in kennis worden gesteld en heeft deze dus de mogelijkheid om het verzoek bij de rechter aan te vechten. Zie ook het overzicht in Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (ministerie van Justitie: Doorzoeking en inbeslagneming van computers en verkrijging van elektronisch bewijs in strafonderzoeken), hoofdstuk 3: The Stored Communications Act, blz. 115-138.

([190]) Volgens de verklaringen van de Amerikaanse overheid 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. Zie de verklaringen van het ministerie van Justitie (bijlage VII), blz. 2.

(129) Hetzelfde geldt voor het gebruik van administratieve dwangbevelen voor doeleinden van openbaar belang. Bovendien gelden er, volgens de verklaringen van de Amerikaanse overheid, soortgelijke materiële beperkingen, omdat diensten alleen toegang mogen trachten te verkrijgen tot gegevens die relevant zijn voor aangelegenheden die binnen hun bevoegdheid vallen en de maatstaf van redelijkheid moeten eerbiedigen.

(130) Bovendien voorziet de Amerikaanse wetgeving in een aantal gerechtelijke verhaalsmogelijkheden voor natuurlijke personen tegen een overheidsinstantie of een van haar functionarissen, wanneer die instantie persoonsgegevens verwerkt. Die verhaalsmogelijkheden, onder meer op grond van de Administrative Procedure Act, de Freedom of Information Act en de Electronic Communications Privacy Act, staan open voor alle natuurlijke personen, ongeacht hun nationaliteit, onder de toepasselijke voorwaarden.

(131) De Administrative Procedure Act voorziet algemeen in gerechtelijke verhaalsmogelijkheden ([191]), 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 ([192]). 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 ([193]).

(132) Meer specifiek wordt in titel II van de Electronic Communications Privacy Act ([194]) 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 ([195]). 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.

(133) Daarnaast heeft eenieder op grond van de Freedom of Information Act (5 U.S.C. § 552) het recht om toegang te krijgen tot gegevens van federale instanties en om, na uitputting van de administratieve procedures, dat recht gerechtelijk te doen handhaven, tenzij die gegevens tegen openbaarmaking zijn beschermd op grond van een vrijstelling of een bijzondere uitzondering ten behoeve van de rechtshandhaving ([196]).

([191]) 5 U.S.C. § 702.

([192]) 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.

([193]) 5 U.S.C. § 706(2)(A).

([194]) 18 U.S.C. §§ 2701-2712.

([195]) 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.

([196]) Die uitzonderingen zijn echter afgebakend. De rechten uit hoofde van de Freedom of Information Act gelden op grond van 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)).

(134) 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 ([197]), de Computer Fraud and Abuse Act ([198]), de Federal Torts Claim Act ([199]), de Right to Financial Privacy Act ([200]) en de Fair Credit Reporting Act ([201]).

(135) De Commissie concludeert derhalve dat er in de Verenigde Staten regelgeving bestaat die bedoeld is om ingrepen ten behoeve van de rechtshandhaving ([202]) en andere doeleinden van openbaar belang in de grondrechten van de personen van wie de gegevens uit de Unie naar de Verenigde Staten worden doorgegeven in het kader van het EU-VS-privacyschild, te beperken tot hetgeen strikt noodzakelijk is om de betrokken legitieme doelstelling te bereiken, en die een doeltreffende rechtsbescherming tegen dergelijke inmenging waarborgt.

4. PASSEND BESCHERMINGSNIVEAU OP GROND VAN HET EU-VS-PRIVACYSCHILD

(136) In het licht van deze bevindingen is de Commissie van oordeel dat door de Verenigde Staten een passend beschermingsniveau wordt gewaarborgd voor de doorgifte van persoonsgegevens uit de Unie naar organisaties met een zelfcertificering in de Verenigde Staten in het kader van het EU-VS-privacyschild.

(137) De Commissie is met name van oordeel dat de Beginselen die door het Amerikaanse ministerie van Handel zijn gepubliceerd, in hun geheel een beschermingsniveau van persoonsgegevens waarborgen dat in grote lijnen overeenkomt met het beschermingsniveau dat wordt gewaarborgd door de in Richtlijn 95/46/EG vastgestelde beginselen.

(138) Daarnaast wordt de doeltreffende toepassing van de Beginselen gewaarborgd door de transparantieverplichtingen en het beheer van het privacyschild door het ministerie van Handel.

(139) Bovendien is de Commissie van oordeel dat, als geheel genomen, de toezichts- en verhaalsmechanismen waarin het privacyschild voorziet, het mogelijk maken om inbreuken op de Beginselen door privacyschildorganisaties in de praktijk vast te stellen en te bestraffen, en de betrokkene rechtsmiddelen bieden om toegang te krijgen tot de hem betreffende persoonsgegevens en, uiteindelijk, om deze gegevens te laten corrigeren of wissen.

(140) Tot slot is de Commissie van oordeel, op basis van de beschikbare informatie over de Amerikaanse rechtsorde, met inbegrip van de verklaringen en toezeggingen van de Amerikaanse overheid, dat ingrepen door de Amerikaanse overheidsdiensten in de grondrechten van de personen van wie de persoonsgegevens in het kader van het privacyschild uit de Unie naar de Verenigde Staten worden doorgegeven, ten behoeve van de nationale veiligheid, de rechtshandhaving of andere doeleinden van openbaar belang, en de daaruit voortvloeiende beperkingen die aan organisaties met een zelfcertificering met betrekking tot de Beginselen worden opgelegd, zullen worden beperkt tot hetgeen strikt noodzakelijk is om de betrokken legitieme doelstelling te bereiken, en dat er doeltreffende rechtsbescherming tegen dergelijke ingrepen bestaat.

([197]) 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 adressen en 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).

([198]) 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.

([199]) 28 U.S.C. §§ 2671 et seq. 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".

([200]) 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.

([201]) 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.

([202]) Het Hof van Justitie heeft erkend dat rechtshandhaving een legitieme beleidsdoelstelling is. Zie arrest van het Hof van Justitie van 8 april 2014, Digital Rights Ireland e.a., gevoegde zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238, punt 42. Zie ook artikel 8, lid 2, van het Europees Verdrag tot bescherming van de rechten van de mens en het arrest van het Europees Hof voor de rechten van de mens van 29 juni 2006, Weber en Saravia/Duitsland, verzoekschrift nr. 54934/00, punt 104.

(141) De Commissie concludeert dat hiermee wordt voldaan aan de normen van artikel 25 van Richtlijn 95/46/EG, geïnterpreteerd in het licht van het Handvest van de grondrechten van de Europese Unie, zoals uitgelegd door het Hof van Justitie in met name het arrest Schrems.

5. MAATREGELEN VAN GEGEVENSBESCHERMINGSAUTORITEITEN EN INFORMATIE AAN DE COMMISSIE

(142) In het arrest Schrems heeft het Hof van Justitie verduidelijkt dat de Commissie niet bevoegd is om de bevoegdheden die de gegevensbeschermingsautoriteiten aan artikel 28 van Richtlijn 95/46/EG ontlenen (met inbegrip van de bevoegdheid om gegevensdoorgiften op te schorten), te beperken wanneer een persoon, bij het instellen van een vordering krachtens die bepaling, de verenigbaarheid van een adequaatheidsbesluit van de Commissie met de bescherming van het grondrecht op privacy en de bescherming van persoonsgegevens in twijfel trekt ([203]).

(143) Om doeltreffend te kunnen controleren of het privacyschild goed functioneert, moet de Commissie door de lidstaten worden geïnformeerd over relevante maatregelen van de gegevensbeschermingsautoriteiten.

(144) Het Hof van Justitie heeft voorts geoordeeld dat de lidstaten en hun organen overeenkomstig artikel 25, lid 6, tweede alinea, van Richtlijn 95/46/EG de noodzakelijke maatregelen moeten nemen om zich naar de besluiten van de EU-instellingen te voegen, aangezien deze in beginsel worden geacht rechtmatig te zijn en derhalve rechtsgevolgen hebben totdat ze worden ingetrokken, nietig verklaard in een beroep tot nietigverklaring of ongeldig verklaard na een verzoek om een prejudiciële beslissing of een exceptie van onwettigheid. Daarom is een krachtens artikel 25, lid 6, van Richtlijn 95/46/EG vastgesteld adequaatheidsbesluit van de Commissie bindend voor alle organen van de lidstaten waaraan het is gericht, met inbegrip van hun onafhankelijke toezichthoudende autoriteiten ([204]). Indien een dergelijke autoriteit een klacht heeft ontvangen waarin de conformiteit van een adequaatheidsbesluit van de Commissie met de bescherming van het grondrecht op privacy en gegevensbescherming in twijfel wordt getrokken, en van oordeel is dat de grieven gegrond zijn, moet het nationale recht voorzien in een rechtsmiddel om deze grieven aan een nationale rechter voor te leggen die, bij twijfel, de behandeling moet schorsen en bij prejudiciële verwijzing het Hof van Justitie om beoordeling van de geldigheid moet verzoeken ([205]).

6. PERIODIEKE EVALUATIE VAN DE VASTSTELLING VAN DE ADEQUAATHEID

(145) In het licht van het feit dat het door de Amerikaanse rechtsorde geboden beschermingsniveau aan wijzigingen onderhevig kan zijn, zal de Commissie, na de vaststelling van dit besluit, periodiek controleren of de vaststellingen met betrekking tot de adequaatheid van het beschermingsniveau dat door de Verenigde Staten in het kader van het EU-VS-privacyschild wordt gewaarborgd, nog steeds feitelijk en rechtens gerechtvaardigd zijn. Een dergelijke controle is in elk geval vereist wanneer de Commissie informatie ontvangt die aanleiding geeft tot gerechtvaardigde twijfel dienaangaande ([206]).

(146) Daarom zal de Commissie het algemene kader van het EU-VS-privacyschild voor de doorgifte van persoonsgegevens, evenals de naleving door de Amerikaanse autoriteiten van de verklaringen en toezeggingen in de aan dit besluit gehechte documenten, voortdurend controleren. Om dit proces te vergemakkelijken, hebben de Verenigde Staten toegezegd om de Commissie te informeren over materiële ontwikkelingen in de Amerikaanse wetgeving op het gebied van gegevensbescherming, wanneer die relevant zijn voor het privacyschild, en in de beperkingen en waarborgen die gelden voor de toegang tot persoonsgegevens door overheidsinstanties. Bovendien zal dit besluit worden onderworpen aan een jaarlijkse gezamenlijke evaluatie die alle aspecten van de werking van het EU-VS-privacyschild zal beslaan, met inbegrip van het effect van de uitzonderingen ten behoeve van de nationale veiligheid en de rechtshandhaving op de Beginselen. Omdat de vaststelling van adequaatheid ook door juridische ontwikkelingen in het Unierecht kan worden beïnvloed, zal de Commissie daarnaast het door het privacyschild geboden beschermingsniveau beoordelen na de inwerkingtreding van de algemene verordening gegevensbescherming.

(147) Voor de uitvoering van de in de bijlagen I, II en III bedoelde jaarlijkse gezamenlijke evaluatie zal de Commissie bijeenkomen met het ministerie van Handel en de FTC, in voorkomend geval vergezeld van andere ministeries en diensten die bij de uitvoering van het privacyschildregeling betrokken zijn, maar ook, voor aangelegenheden in verband met de nationale veiligheid, met vertegenwoordigers van het ODNI, andere onderdelen van de inlichtingendiensten en de ombudsman. De deelname aan deze vergadering zal openstaan voor Europese gegevensbeschermingsautoriteiten en vertegenwoordigers van de Artikel 29-werkgroep.

([203]) Arrest Schrems, punten 40 e.v., 101-103.
([204]) Arrest Schrems, punten 51, 52 en 62.
([205]) Arrest Schrems, punt 65.
([206]) Arrest Schrems, punt 76.

(148) In het kader van de jaarlijkse gezamenlijke evaluatie zal de Commissie vragen dat het ministerie van Handel uitgebreide informatie verstrekt over alle relevante aspecten van de werking van het EU-VS-privacyschild, met inbegrip van door het ministerie van Handel ontvangen verwijzingen van gegevensbeschermingsautoriteiten en de resultaten van ambtshalve nalevingscontroles. De Commissie zal ook uitleg vragen met betrekking tot eventuele vragen of aangelegenheden inzake het EU-VS-privacyschild en de werking ervan die voortvloeien uit beschikbare informatie, waaronder de transparantieverslagen waarin de USA Freedom Act voorziet, openbare verslagen van de Amerikaanse inlichtingendiensten, de gegevensbeschermingsautoriteiten, privacyorganisaties, berichten in de media of alle andere mogelijke bronnen. Bovendien moeten de lidstaten, om de taak van de Commissie in dit verband te vergemakkelijken, de Commissie informeren over gevallen waarin de maatregelen van de instanties die verantwoordelijk zijn om de naleving van de Beginselen in de Verenigde Staten te waarborgen, die naleving niet waarborgen, en over eventuele aanwijzingen dat de maatregelen van de Amerikaanse overheidsdiensten die verantwoordelijk zijn voor de nationale veiligheid of de preventie, het onderzoek, de opsporing of de vervolging van strafbare feiten, het vereiste beschermingsniveau niet waarborgen.

(149) Op basis van de jaarlijkse gezamenlijke evaluatie zal de Commissie een openbaar verslag opstellen dat bij het Europees Parlement en de Raad moet worden ingediend.

7. **SCHORSING VAN HET ADEQUAATHEIDSBESLUIT**

(150) Wanneer de Commissie concludeert, op basis van de controles of andere beschikbare informatie, dat het door het privacyschild geboden beschermingsniveau niet langer kan worden geacht in grote lijnen overeen te komen met het beschermingsniveau in de Unie, of wanneer er duidelijke aanwijzingen zijn dat doeltreffende naleving van de Beginselen in de Verenigde Staten niet langer kan worden gewaarborgd, of dat de maatregelen van de Amerikaanse overheidsdiensten die verantwoordelijk zijn voor de nationale veiligheid of de preventie, het onderzoek, de opsporing of de vervolging van strafbare feiten, het vereiste beschermingsniveau niet waarborgen, stelt zij het ministerie van Handel daarvan op de hoogte en verzoekt zij om passende maatregelen te nemen om een potentiële niet-naleving van de Beginselen snel aan te pakken binnen een vastgestelde, redelijke termijn. Indien de Amerikaanse autoriteiten na het verstrijken van de vastgestelde termijn niet afdoende kunnen aantonen dat het EU-VS-privacyschild doeltreffende naleving en een passend beschermingsniveau blijft waarborgen, zal de Commissie de procedure in gang zetten die moet leiden tot de gedeeltelijke of volledige schorsing of intrekking van dit besluit ([207]). Als alternatief kan de Commissie voorstellen dit besluit te wijzigen, bijvoorbeeld door de reikwijdte van de vaststelling van adequaatheid te beperken tot alleen gegevensdoorgiften waaraan aanvullende voorwaarden worden verbonden.

(151) De Commissie zal met name de procedure tot schorsing of intrekking in gang zetten indien:

a) er aanwijzingen zijn dat de Amerikaanse autoriteiten de verklaringen en toezeggingen in de aan dit besluit gehechte documenten niet nakomen, onder meer ten aanzien van de voorwaarden voor en beperkingen van de toegang van de Amerikaanse overheidsdiensten ten behoeve van de nationale veiligheid, de rechtshandhaving en andere doeleinden van openbaar belang tot in het kader van het privacyschild doorgegeven persoonsgegevens;

b) klachten van betrokkenen uit de EU niet doeltreffend worden behandeld; in dit verband zal de Commissie rekening houden met alle omstandigheden die van invloed zijn op de mogelijkheid voor betrokkenen uit de EU om hun rechten te laten gelden, met inbegrip van met name de vrijwillige toezegging van Amerikaanse ondernemingen met een zelfcertificering tot samenwerking met de gegevensbeschermingsautoriteiten en opvolging van hun advies; of

c) de privacyschildombudsman niet tijdig en passend reageert op de verzoeken van betrokkenen uit de EU.

(152) De Commissie zal ook de procedure die tot de wijziging, schorsing of intrekking van dit besluit leidt, overwegen indien, in het kader van de jaarlijkse gezamenlijke evaluatie van de werking van het EU-VS-privacyschild of anders, het ministerie van Handel of andere ministeries of diensten die betrokken zijn bij de tenuitvoerlegging van het privacyschild of, voor aangelegenheden in verband met de nationale veiligheid, vertegenwoordigers van de Amerikaanse inlichtingendiensten of de ombudsman, nalaten de informatie of toelichtingen te verstrekken die nodig zijn voor de beoordeling van de naleving van de Beginselen, de doeltreffendheid van de procedures voor de behandeling van klachten of een verlaging van het vereiste beschermingsniveau als gevolg van maatregelen van de

([207]) Vanaf de datum van toepassing van de algemene verordening gegevensbescherming zal de Commissie gebruikmaken van haar bevoegdheid tot vaststelling, om naar behoren gerechtvaardigde dwingende urgente redenen, van een uitvoeringshandeling tot schorsing van dit besluit, die onmiddellijk van toepassing is zonder voorafgaande voorlegging aan het bevoegde comitologiecomité en die gedurende ten hoogste zes maanden van kracht blijft.

Amerikaanse inlichtingendiensten, met name als gevolg van de verzameling van en/of de toegang tot persoonsgegevens die niet beperkt is tot hetgeen strikt noodzakelijk en evenredig is. In dit verband zal de Commissie rekening houden met de mate waarin de relevante informatie kan worden verkregen uit andere bronnen, zoals via verslagen van Amerikaanse ondernemingen met een zelfcertificering zoals toegestaan op grond van de USA Freedom Act.

(153) De bij artikel 29 van Richtlijn 95/46/EG opgerichte Groep betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens heeft over het beschermingsniveau dat door het EU-VS-privacyschild wordt geboden ([208]), adviezen uitgebracht waarmee bij de voorbereiding van dit besluit rekening is gehouden.

(154) Het Europees Parlement heeft een resolutie over trans-Atlantische gegevensstromen aangenomen ([209]).

(155) De in dit besluit vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 31, lid 1, van Richtlijn 95/46/EG ingestelde comité,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

1. oor de toepassing van artikel 25, lid 2, van Richtlijn 95/46/EG waarborgen de Verenigde Staten een passend beschermingsniveau voor persoonsgegevens die van de Unie naar organisaties in de Verenigde Staten worden doorgegeven in het kader van het EU-VS-privacyschild.

2. Het EU-VS-privacyschild bestaat uit de Beginselen die op 7 juli 2016 door het Amerikaanse ministerie van Handel zijn gepubliceerd en in bijlage II zijn opgenomen, en de officiële verklaringen en toezeggingen die in de in de bijlagen I en III tot en met VII opgenomen documenten zijn vervat.

3. Voor de toepassing van lid 1 worden persoonsgegevens doorgegeven in het kader van het EU-VS-privacyschild wanneer ze worden doorgegeven uit de Unie naar organisaties in de Verenigde Staten die op de „privacyschildlijst" staan, die door het Amerikaanse ministerie van Handel wordt bijgehouden en bekendgemaakt, overeenkomstig de secties I en III van de in bijlage II opgenomen Beginselen.

Artikel 2

De toepassing van de bepalingen van Richtlijn 95/46/EG, met uitzondering van artikel 25, lid 1, die betrekking hebben op de verwerking van persoonsgegevens in de lidstaten, en met name artikel 4, wordt door dit besluit onverlet gelaten.

Artikel 3

Wanneer de bevoegde autoriteiten in de lidstaten hun bevoegdheden uit hoofde van artikel 28, lid 3, van Richtlijn 95/46/EG uitoefenen, en dit tot de opschorting van of een definitief verbod op gegevensstromen naar een organisatie in de Verenigde Staten die op de privacyschildlijst staat overeenkomstig de secties I en III van de in bijlage II opgenomen Beginselen leidt, teneinde natuurlijke personen met betrekking tot de verwerking van hun persoonsgegevens te beschermen, stelt de betrokken lidstaat de Commissie hiervan onverwijld in kennis.

Artikel 4

1. De Commissie zal de werking van het EU-VS-privacyschild voortdurend controleren om te beoordelen of de Verenigde Staten een passend beschermingsniveau blijven waarborgen voor de in het kader daarvan uit de Unie naar organisaties in de Verenigde Staten doorgegeven persoonsgegevens.

([208]) Advies 01/2016 over het ontwerp-adequaatheidsbesluit over het EU-VS-privacyschild, aangenomen op 13 april 2016.
([209]) Resolutie van het Europees Parlement van 26 mei 2016 over trans-Atlantische gegevensstromen (2016/2727(RSP)).

2. De lidstaten en de Commissie stellen elkaar in kennis van de gevallen waarin de overheidsinstanties in de Verenigde Staten met de wettelijke bevoegdheid om de in bijlage II opgenomen Beginselen te doen naleven, niet voorzien in doeltreffende opsporings- en toezichtsmechanismen waarmee inbreuken op de 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 strikt noodzakelijk is, en/of dat er geen doeltreffende rechtsbescherming tegen dergelijke ingrepen is.

4. Binnen één jaar na de datum van kennisgeving van dit besluit aan de lidstaten en daarna elk jaar, 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 in de bijlagen I, II en VI bedoelde jaarlijkse gezamenlijke evaluatie is ontvangen.

5. De Commissie zal alle relevante vaststellingen aan het bij artikel 31 van Richtlijn 95/46/EG ingestelde comité meedelen.

6. De Commissie zal volgens de in artikel 31, lid 2, van Richtlijn 95/46/EG bedoelde procedure ontwerpmaatregelen indienen teneinde dit besluit op te schorsen, te wijzigen of in te trekken of het toepassingsgebied ervan te beperken, onder andere, wanneer er aanwijzingen zijn:

— dat de Amerikaanse overheidsdiensten de verklaringen en toezeggingen in de aan dit besluit gehechte documenten niet nakomen, onder meer wat betreft de voorwaarden voor en beperkingen van de toegang van Amerikaanse overheidsdiensten ten behoeve van de nationale veiligheid, de rechtshandhaving en andere doeleinden van openbaar belang tot in het kader van het EU-VS-privacyschild doorgegeven persoonsgegevens;

— dat klachten van betrokkenen uit de EU stelselmatig niet doeltreffend worden behandeld; of

— dat de privacyschildombudsman stelselmatig niet tijdig en passend reageert op verzoeken van betrokkenen uit de EU, zoals in sectie 4(e) van bijlage III wordt vereist.

De Commissie zal dergelijke ontwerpmaatregelen ook indienen indien zij door het gebrek aan medewerking van de instanties die bij het waarborgen van de werking van het EU-VS-privacyschild in de Verenigde Staten betrokken zijn, niet kan bepalen of de vaststelling in artikel 1, lid 1, in het gedrang komt.

Artikel 5

De lidstaten nemen alle nodige maatregelen om aan dit besluit te voldoen.

Artikel 6

Dit besluit is gericht tot de lidstaten.

Gedaan te Brussel, 12 juli 2016.

Voor de Commissie
Věra JOUROVÁ
Lid van de Commissie

BIJLAGE I

Brief van de Amerikaanse minister van Handel Penny Pritzker

7 juli 2016

Mw. Věra Jourová
Commissaris voor Justitie, Consumentenzaken en Gendergelijkheid
Europese Commissie
Wetstraat 200
1049 Brussel
BELGIË

Geachte commissaris Jourová:

Namens de Verenigde Staten heb ik de eer u hierbij te doen toekomen een pakket documenten inzake het EU-VS-privacyschild dat het resultaat is van twee jaar productieve besprekingen tussen onze teams. Dit pakket biedt, samen met andere documenten waarover de Commissie de beschikking heeft via openbare bronnen, een zeer sterke basis voor een nieuwe vaststelling van gepastheid door de Europese Commissie ([1]).

We kunnen beiden trots zijn op de verbeteringen in de kaderregeling. Het privacyschild is gebaseerd op Beginselen die aan beide kanten van de Atlantische Oceaan een brede steun genieten, en wij hebben de werking van deze beginselen versterkt. Door samen te werken, hebben wij een reële kans om de bescherming van de privacy in de hele wereld te beschermen.

Het privacyschildpakket omvat de Beginselen inzake het privacyschild, alsook een brief, opgenomen als bijlage 1, van de Dienst voor Internationale Handel van het ministerie van Handel, die het programma beheert. Hierin worden de toezeggingen beschreven die onze ministerie heeft gedaan om ervoor te zorgen dat het privacyschild effectief functioneert. Bijlage 2 bij het pakket bevat onder andere toezeggingen van het ministerie van Handel met betrekking tot het nieuwe arbitrale model in het kader van het privacyschild.

Ik heb mijn ambtenaren opdracht gegeven alle nodige middelen in te zetten om het kader van het privacyschild snel en volledig in te voeren en ervoor te zorgen dat op tijd aan de in bijlage 1 en bijlage 2 neergelegde verplichtingen wordt voldaan.

Het privacyschildpakket bevat tevens documenten van andere Amerikaanse instanties, namelijk:

— een brief van de Federal Trade Commission (FTC) waarin de tenuitvoerlegging van het privacyschild wordt beschreven;

— een brief van het ministerie van Vervoer waarin zijn tenuitvoerlegging van het privacyschild wordt beschreven;

— twee door het bureau van de directeur van de nationale inlichtingendienst (ODNI) opgestelde brieven met betrekking tot waarborgen en beperkingen die van toepassing zijn op de nationale veiligheidsautoriteiten van de VS;

— een brief van het Amerikaanse ministerie van Buitenlands Zaken en een bijbehorend memorandum, waarin de toezegging van het ministerie van Buitenlandse Zaken wordt beschreven met betrekking tot het instellen van een nieuwe privacyschildombudsman voor het indienen van vragen met betrekking tot de Amerikaanse „signal intelligence”-praktijken, 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.

U kunt ervan verzekerd zijn dat de Verenigde Staten deze toezeggingen ernstig neemt.

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

Binnen 30 dagen na de definitieve goedkeuring van de vaststelling van het beschermingsniveau wordt het volledige privacyschildpakket ingediend bij het Federal Register voor de bekendmaking ervan.

Wij kijken ernaar uit met u samen te werken wanneer het privacyschild is geïmplementeerd en we samen aan de volgende fase van dit proces beginnen.

Met vriendelijke groet,

Penny Pritzker

Bijlage 1

Brief van de waarnemend onderminister van Internationale Handel Ken Hyatt

Mevrouw Věra Jourová
Commissaris voor Justitie, Consumentenrechten en Gendergelijkheid
Europese Commissie
Westraat 200
1049 Brussel
BELGIË

Geachte commissaris Jourová:

Namens de Dienst voor Internationale Handel heb ik de eer u een beschrijving te geven van de verbeterde bescherming van persoonsgegevens die het EU-VS-privacyschildkader („privacyschild" of „kader") biedt, en van de toezeggingen die het ministerie van Handel („ministerie") heeft gedaan om ervoor te zorgen dat het privacyschild effectief functioneert. De voltooiing van deze historische regeling is een belangrijk resultaat voor de privacy en het bedrijfsleven aan beide zijden van de Atlantische Oceaan. Het privacyschild biedt EU-burgers het vertrouwen dat hun gegevens worden beschermd en dat zij over rechtsmiddelen beschikken om eventuele problemen aan te pakken. Het biedt zekerheid die de trans-Atlantische economie zal helpen groeien door ervoor te zorgen dat duizenden Europese en Amerikaanse ondernemingen over onze grenzen heen kunnen blijven investeren en zakendoen. Het privacyschild is het resultaat van ruim twee jaar hard werk en samenwerking met u, onze collega's binnen de Europese Commissie („Commissie"). Wij verheugen ons erop te blijven samenwerken met de Commissie om ervoor te zorgen dat het privacyschild blijft werken zoals bedoeld.

Samen met de Commissie hebben we het privacyschild ontwikkeld zodat in de Verenigde Staten gevestigde organisaties kunnen voldoen aan de eisen inzake gepastheid inzake gegevensbescherming in het kader van EU-wetgeving. De nieuwe kaderregeling zal een aantal aanzienlijke voordelen opleveren voor zowel particulieren als bedrijven. Ten eerste biedt het een belangrijke reeks privacybeschermingen voor de gegevens van EU-burgers. Het vereist dat de deelnemende organisaties in de VS een conform privacybeleid ontwikkelen, in het openbaar toezeggen te zullen voldoen aan de privacyschildbeginselen, zodat de nakoming van de toezegging kan worden afgedwongen, jaarlijks hun naleving bij het ministerie hercertificeren, gratis onafhankelijke geschillenbeslechting aan EU-burgers aanbieden, en onderworpen zijn aan het gezag van de Amerikaanse Federal Trade Commission („FTC"), het ministerie van Vervoer („DOT"), of een andere handhavingsinstantie. Ten tweede zal het privacyschild duizenden bedrijven in de Verenigde Staten en 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 trans-Atlantische economische relatie is reeds 's werelds grootste, goed voor de helft van de wereldwijde economische output en bijna een biljoen dollar aan goederen en dienstenhandel, waarmee miljoenen banen aan beide zijden van de Atlantische Oceaan worden ondersteund. 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 (KMO's). 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 privacyschild ondersteunt gedeelde privacybeginselen, waarbij de verschillen in onze juridische aanpak worden overbrugd, en tevens de handels- en economische doelstellingen van zowel Europa als de Verenigde Staten worden bevorderd.

Het besluit van een bedrijf om zichzelf voor dit nieuwe kader te certificeren is vrijwillig. Zodra echter een bedrijf zich publiekelijk tot het privacyschild verplicht, is de naleving van deze verplichting afdwingbaar krachtens de Amerikaanse wetgeving, hetzij door de Federal Trade Commission hetzij door het ministerie van Vervoer, afhankelijk van welke instantie bevoegdheid over de privacyschildorganisatie uitoefent.

Verbeteringen in het kader van de privacyschildbeginselen

Het uiteindelijke privacyschild versterkt de bescherming van de privacy door:

— te eisen dat aanvullende informatie wordt verstrekt aan burgers in het kader van het kennisgevingsbeginsel, met inbegrip van een verklaring van deelname van de organisatie aan het privacyschild, een verklaring van het recht van de burger om toegang te krijgen tot persoonsgegevens en de aanwijzing van het desbetreffende onafhankelijke orgaan van geschillenbeslechting;

— versterking van de bescherming van de persoonsgegevens die een privacyschildorganisatie aan een derde voor de verwerking verantwoordelijke overdraagt, door te eisen dat de partijen een overeenkomst aangaan die bepaalt dat dergelijke gegevens alleen mogen worden verwerkt voor beperkte en bepaalde doeleinden die met de door de burger verleende toestemming overeenstemmen, en dat de begunstigde dezelfde mate van bescherming zal bieden als de Beginselen;

— versterking van de bescherming van persoonsgegevens die een privacyschildorganisatie aan vertegenwoordigers van derde partijen overdraagt, door onder andere te eisen dat een privacyschildorganisatie: redelijke en passende maatregelen neemt om ervoor te zorgen dat de externe vertegenwoordiger de overgedragen persoonsgegevens verwerkt op een wijze die in overeenstemming is met de verplichtingen van de organisatie in het kader van de Beginselen; na kennisgeving, redelijke en passende maatregelen neemt om ongeoorloofde verwerking te stoppen en te herstellen; een samenvatting of een representatief exemplaar van de desbetreffende privacybepalingen van de overeenkomst met die externe vertegenwoordiger op verzoek aan het ministerie overlegt;

— te bepalen dat een privacyschildorganisatie verantwoordelijk is voor de verwerking van persoonsgegevens die zij in het kader van het privacyschild ontvangt en vervolgens overdraagt aan een derde die namens haar optreedt, en dat de privacyschildorganisatie op grond van de Beginselen aansprakelijk blijft als haar vertegenwoordiger dergelijke persoonsgegevens verwerkt op een wijze die niet in overeenstemming is met de Beginselen, tenzij de organisatie bewijst dat zij niet verantwoordelijk is voor de gebeurtenis die aanleiding geeft tot de schade;

— te verduidelijken dat privacyschildorganisaties de persoonsgegevens moeten beperken tot de informatie die met het oog op de verwerking relevant is;

— te eisen dat een organisatie elk jaar bij het ministerie certificeert dat zij zich ertoe verplicht de Beginselen toe te passen op de informatie die zij heeft ontvangen terwijl zij aan het privacyschild deelnam indien zij het privacyschild verlaat en ervoor kiest om dergelijke gegevens te bewaren;

— te eisen dat in onafhankelijke verhaalmechanismen wordt voorzien zonder kosten voor de burger;

— te eisen dat zowel organisaties als hun geselecteerde onafhankelijke verhaalmechanismen onmiddellijk moeten reageren op vragen en informatieverzoeken van het ministerie van Informatie in verband met het privacyschild;

— te eisen dat organisaties snel reageren op klachten over de naleving van de Beginselen die de autoriteiten van de EU-lidstaten via het ministerie hebben ingediend; en

— te eisen dat een privacyschildorganisatie alle desbetreffende privacyschildgerelateerde secties van elk aan de FTC voorgelegd nalevings- or beoordelingsverslag openbaar maakt indien zij onderworpen wordt aan een FTC- of rechterlijk bevel op grond van niet-naleving.

Beheer en toezicht inzake het privacyschildprogramma door het ministerie van Handel

Het ministerie herhaalt zijn toezegging dat het een gezaghebbende lijst zal bijhouden en ter beschikking van het publiek zal stellen van Amerikaanse organisaties die bij het ministerie een zelfcertificeringsverklaring hebben ingediend en zich hebben verplicht om zich aan de Beginselen te houden (de „privacyschildlijst"). Het ministerie houdt de privacyschildlijst actueel door organisaties te verwijderen die zich vrijwillig terugtrekken, die niet aan de jaarlijkse hercertificering overeenkomstig de procedures van het ministerie voldoen, of die permanent nalaten aan de regels te voldoen. Het ministerie zal tevens een gezaghebbende lijst bijhouden en ter beschikking van het publiek zal stellen van Amerikaanse organisaties die eerder wel bij het ministerie een zelfcertificeringsverklaring hadden ingediend, maar die van de privacyschildlijst zijn verwijderd, met inbegrip van de organisaties die werden verwijderd wegens permanente niet-naleving van de Beginselen. Het ministerie zal de redenen opgeven waarom een organisatie werd verwijderd.

Daarnaast verbindt het ministerie zich ertoe het beheer en het toezicht inzake het privacyschild te versterken. In het bijzonder zal het ministerie:

Aanvullende informatie over de privacyschildwebsite verstrekken

— de privacyschildlijst bijhouden, evenals een overzicht van de organisaties die voorheen een zelfcertificeringsverklaring indienden met betrekking tot de naleving van de Beginselen, maar die niet meer verzekerd zijn van de voordelen van het privacyschild;

— op een prominente plaats een toelichting opnemen waarin duidelijk wordt gemaakt dat alle organisaties die van de privacyschildlijst zijn verwijderd niet meer verzekerd zijn van de voordelen van het privacyschild, maar desalniettemin de Beginselen moeten blijven toepassen op de persoonsgegevens die zij ontvingen toen zij deelnamen aan het privacyschild zolang zij deze gegevens bewaren; en

— een link verschaffen naar de lijst van privacyschildgerelateerde FTC-zaken die wordt bijgehouden op de FTC-website.

De inachtneming van de vereisten inzake zelfcertificering controleren

— Voorafgaand aan de afronding van de zelfcertificering (of jaarlijkse hercertificering) van een organisatie en het plaatsen van een organisatie op de privacyschildlijst, wordt gecontroleerd of de organisatie:

  — de benodigde contactgegevens van de organisatie heeft verstrekt;

  — de activiteiten van de organisatie heeft beschreven met betrekking tot de uit de EU ontvangen persoonsgegevens;

  — heeft aangegeven op welke persoonsgegevens haar zelfcertificering betrekking heeft;

  — indien zij een publiek toegankelijke website heeft, het internetadres waar het privacybeleid beschikbaar is, heeft verstrekt, en of het privacybeleid toegankelijk is op het verstrekte webadres, of als een organisatie geen publiek toegankelijke website heeft, zij heeft aangegeven waar het publiek het privacybeleid kan inzien;

  — in haar desbetreffende privacybeleid een verklaring dat zij de Beginselen naleeft en, als het privacybeleid online beschikbaar is, een hyperlink naar de privacyschildwebsite van het ministerie heeft opgenomen;

  — de officiële instantie heeft aanwezen 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 is opgenomen in de Beginselen of een toekomstige bijlage bij de Beginselen);

  — indien zij ervoor kiest om de eisen in de punten (a)(i) en (a)(iii) van het Beginsel inzake verhaal, handhaving en aansprakelijkheid na te leven door zich te verplichten om met de bevoegde EU-gegevensbeschermingsautoriteiten samen te werken, heeft aangegeven dat zij de intentie heeft om samen te werken met de gegevensbeschermingsautoriteiten bij het onderzoek en de oplossing van klachten die in het kader van de privacyschild zijn ingediend en met name om te reageren op vragen van EU-betrokkenen wanneer zij hun klachten rechtstreeks bij hun nationale gegevensbeschermingsautoriteiten hebben ingediend;

  — een privacyprogramma heeft aangewezen waarvan de organisatie lid is;

  — de wijze heeft aangegeven waarop wordt gecontroleerd of de Beginselen daadwerkelijk worden nageleefd (bv. intern, door derden);

  — zowel in haar zelfcertificeringsverklaring als in haar privacybeleid het onafhankelijke verhaalsmechanisme heeft aangegeven waarmee klachten kunnen worden onderzocht en opgelost;

  — in haar desbetreffende privacybeleid, indien dat beleid online beschikbaar is, een hyperlink heeft opgenomen naar de website of het klachtenformulier van het onafhankelijke verhaalsmechanisme dat beschikbaar is om onopgeloste klachten te onderzoeken; en

  — indien zij heeft aangegeven dat zij voornemens is personeelsbeheersinformatie te ontvangen die vanuit de EU is doorgegeven voor gebruik in het kader van de arbeidsverhouding, zich ertoe heeft verplicht samen te werken met en zich te schikken naar de gegevensbeschermingautoriteiten teneinde klachten op te lossen over haar activiteiten met betrekking tot dergelijke gegevens, aan het ministerie een kopie van haar privacybeleid inzake personeelsbeheersinformatie heeft verstrekt en heeft vermeld waar het privacybeleid beschikbaar is voor inzage door haar werknemers die het aangaat.

— Gebruik maken van onafhankelijke verhaalsmechanismen om te controleren of de organisaties daadwerkelijk geregistreerd zijn bij het desbetreffende mechanisme dat in hun zelfcertificeringsverklaring is aangegeven, wanneer een dergelijke registratie is vereist.

De inspanningen opvoeren om organisaties te blijven volgen die van de privacyschildlijst zijn verwijderd

— organisaties die vanwege „permanente niet-naleving” van de privacyschildlijst zijn verwijderd, ervan in kennis stellen dat zij de informatie die in het kader van het privacyschild is verzameld niet mogen bewaren; en

— vragenlijsten toesturen aan organisaties waarvan de zelfcertificering verloopt, of die zich vrijwillig uit het privacyschild hebben teruggetrokken teneinde na te gaan of de organisatie de tijdens haar deelname aan het privacyschild ontvangen persoonsgegevens zal terugbezorgen of wissen, of de privacybeginselen hierop zal blijven toepassen en, indien de persoonsgegevens worden bewaard, na te gaan wie binnen de organisatie het blijvende contactpunt is voor aangelegenheden die met het privacyschild te maken hebben.

Valse beweringen van deelname opsporen en aanpakken

— het privacybeleid herzien van de organisaties die eerder aan het privacyschildprogramma hebben deelgenomen, maar die van de privacyschildlijst zijn verwijderd teneinde de eventuele valsheid van beweringen van deelname aan het privacyschild aan te tonen;

— op een permanente basis, wanneer een organisatie: (a) niet langer deelneemt aan het privacyschild, (b) haar naleving van de Beginselen niet opnieuw certificeert of (c) vanwege met name „permanente niet-naleving" als deelnemer aan het privacyschild wordt verwijderd, ambtshalve controleren of de organisatie alle verwijzingen naar het privacyschild uit het relevante gepubliceerde privacybeleid heeft verwijderd die zouden impliceren dat de organisatie actief blijft deelnemen aan het privacyschild en recht heft op de voordelen ervan. Indien het ministerie vaststelt dat dergelijke verwijzingen niet zijn verwijderd, zal het ministerie de organisatie waarschuwen dat, waar nodig, de zaak naar de desbetreffende autoriteit zal worden verwezen voor eventuele handhavingsmaatregelen als de organisatie blijft verkondigen een privacyschildcertificering te hebben. Als de organisatie noch de verwijzingen verwijdert noch tot een verklaring van zelfcertificering inzake haar naleving in het kader van het privacyschild overgaat, zal het ministerie de zaak ambtshalve verwijzen naar de FTC, minsterie van Handel, of een andere gepaste handhavende instantie of, in voorkomend geval, actie nemen om het privacyschildkeurmerk te handhaven;

— andere inspanningen ondernemen om de valsheid van beweringen inzake deelname aan het privacyschild en oneigenlijk gebruik van het privacyschildkeurmerk vast te stellen, onder meer door middel van zoekopdrachten op internet om vast te stellen waar beelden van het privacyschildkeurmerk worden getoond en in het privacybeleid van organisaties naar het privacyschild wordt verwezen;

— onverwijld eventuele problemen aanpakken die worden vastgesteld bij onze ambtshalve controles inzake valse beweringen van deelname en misbruik van het keurmerk, onder meer door het waarschuwen van organisaties die een verkeerde voorstelling geven van hun deelname aan het privacyschildprogramma zoals hierboven beschreven;

— andere passende corrigerende maatregelen nemen, met inbegrip van eventuele gerechtelijke stappen die het ministerie bevoegd is te nemen en de verwijzing van zaken naar de FTC, het ministerie van Handel, of een andere passende handhavende instelling; en

— klachten over valse beweringen van deelname die worden ontvangen, snel onderzoeken en oplossen.

Het ministerie zal het privacybeleid van organisaties herzien zodat valse beweringen van deelname aan het privacyschild beter kunnen worden aangetoond en aangepakt. Meer bepaald zal het ministerie het privacybeleid herzien van organisaties waarvan de zelfcertificering is vervallen omdat zij hun naleving van de Beginselen niet opnieuw hebben gecertificeerd. Het ministerie zal dit soort onderzoek uitvoeren om te controleren of dergelijke organisaties alle verwijzingen uit hun desbetreffende gepubliceerde privacybeleid hebben verwijderd die impliceren dat de organisatie actief blijft deelnemen aan het privacyschild. Naar aanleiding van dit soort onderzoeken stellen wij vast welke organisaties dergelijke verwijzingen niet hebben verwijderd. Deze organisaties ontvangen een brief van het Office of General Counsel van het ministerie met een waarschuwing dat eventueel handhavend zal worden opgetreden als de verwijzingen niet worden verwijderd. Het ministerie zal vervolgmaatregelen nemen om ervoor te zorgen dat de organisaties de ongepaste verwijzingen verwijderen of hun naleving van de Beginselen opnieuw certificeren. Daarnaast zal het ministerie inspanningen leveren om valsheid aan te tonen van beweringen inzake deelname aan het privacyschild door organisaties die nooit hebben deelgenomen aan het privacyschildprogramma, en zal het met betrekking tot dergelijke organisaties vergelijkbare corrigerende maatregelen nemen.

Periodiek ambtshalve nalevingscontroles en evaluaties van het programma uitvoeren

— voortdurend de effectieve naleving monitoren, onder meer door gedetailleerde vragenlijsten aan deelnemende organisaties toe te sturen om de problemen vast te stellen die vervolgmaatregelen kunnen rechtvaardigen. In het bijzonder zullen deze nalevingscontroles plaatsvinden 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 privacyschild, of c) er geloofwaardige aanwijzingen zijn dat een organisatie niet voldoet aan haar verplichtingen in het kader van het privacyschild. Het ministerie zal, waar nodig, in overleg treden met de bevoegde gegevensbeschermingsautoriteiten over dergelijke nalevingscontroles; en

— periodiek het beheer en toezicht inzake het privacyschildprogramma beoordelen om te waarborgen dat de controle-inspanningen geschikt zijn om nieuwe problemen aan te pakken wanneer die zich voordoen.

Het ministerie heeft de middelen uitgebreid die aan het beheer van en toezicht op het privacyschildprogramma worden besteed, met inbegrip van een verdubbeling van het aantal personeelsleden dat belast is met dat beheer en toezicht. We zullen de nodige middelen blijven toekennen voor dergelijke inspanningen om effectief toezicht op en beheer van het programma te verzekeren.

De privacyschildwebsite aanpassen aan specifieke doelgroepen

Het ministerie zal de privacyschildwebsite aanpassen aan drie doelgroepen: EU-burgers, EU-ondernemingen en Amerikaanse bedrijven. 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 duidelijk uitgelegd: 1) welke rechten het privacyschild 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 privacyschild kunnen vinden. Voor EU-ondernemingen zal het gemakkelijker zijn om te controleren: 1) of een organisatie verzekerd is van de voordelen van het privacyschild; 2) op welke soort informatie de zelfcertificering inzake het privacyschild 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.

De samenwerking met de gegevensbeschermingsautoriteiten opvoeren

Om de mogelijkheden voor samenwerking met de gegevensbeschermingsautoriteiten te verhogen, zal het ministerie een speciale contactpersoon instellen om op te treden als tussenpersoon voor de gegevensbeschermingsautoriteiten. In gevallen waarin een gegevensbeschermingsautoriteit, onder meer naar aanleiding van een klacht van een EU-burger, van mening is dat een organisatie de Beginselen niet naleeft, kan zij contact opnemen met de speciale contactpersoon bij het ministerie om de organisatie nader te laten beoordelen. De contactpersoon zal ook meldingen ontvangen met betrekking tot organisaties die ten onrechte beweren dat ze deelnemen aan het privacyschild, terwijl ze nooit door zelfcertificering de Beginselen hebben onderschreven. De contactpersoon zal de gegevensbeschermingsautoriteiten helpen informatie te zoeken over de zelfcertificering of eerdere deelname aan het programma van een bepaalde organisatie, en de contactpersoon zal vragen van de gegevensbeschermingautoriteit beantwoorden over de naleving van specifieke privacyschildvereisten. Ten tweede zal het ministerie de gegevensbeschermingsautoriteiten voorzien van materiaal met betrekking tot het privacyschild, dat zij op hun eigen websites kunnen plaatsen om de transparantie voor EU-burgers en EU-ondernemingen te vergroten. Het toegenomen bewustzijn ten aanzien van het privacyschild en de rechten en plichten die het creëert moet het gemakkelijker maken bepaalde kwesties in een vroeg stadium te constateren, zodat ze op de juiste wijze kunnen worden aangepakt.

De afhandeling van klachten over niet-naleving vereenvoudigen

De klachten over de niet-naleving door een privacyschildorganisatie van de Beginselen ontvangt het ministerie via de vaste contactpersoon naar wie de gegevensbeschermingsautoriteit de klacht heeft doorverwezen. Het ministerie zal zijn uiterste best doen om de afhandeling van de klacht bij de privacyschildorganisatie te bevorderen. Binnen 90 dagen na ontvangst van de klacht verstrekt het ministerie een update aan de gegevensbeschermingsautoriteit. Om de indiening van dergelijke klachten te vereenvoudigen, voert het ministerie een standaardformulier in dat de gegevensbeschermingautoriteiten bij de daartoe aangewezen contactpersoon van het ministerie kunnen indienen. De speciale contactpersoon houdt zich op de hoogte van alle zaken die de gegevensbeschermingsautoriteiten naar het ministerie hebben verwezen, en het ministerie verstrekt in het hieronder beschreven jaarlijkse evaluatie een verslag met een analyse van alle klachten die zij in het betreffende jaar heeft ontvangen.

In overleg met de Commissie arbitrageprocedures vaststellen en arbiters selecteren

Het ministerie komt zijn verplichtingen op grond van bijlage I na en publiceert de procedures nadat overeenstemming is bereikt.

Gezamenlijk mechanisme voor de evaluatie van het functioneren van het privacyschild

Het ministerie van Handel, de FTC en andere instanties zullen in voorkomend geval jaarlijkse vergaderingen houden met de Commissie, belanghebbende gegevensbeschermingsautoriteiten en de desbetreffende vertegenwoordigers van de Artikel 29-werkgroep, waar het ministerie updates over het privacyschildprogramma zal verstrekken. Tijdens de jaarlijkse vergaderingen wordt onder meer gesproken over actuele kwesties inzake het functioneren, de uitvoering, en de handhaving van en het toezicht op het privacyschild, met inbegrip van de verwijzingen die het ministerie van de autoriteiten voor gegevensbescherming heeft ontvangen, en de resultaten van de ambtshalve uitgevoerde nalevingsbeoordelingen, en eventueel ook over relevante veranderingen van de wetgeving. De eerste jaarlijkse evaluatie en de daarop volgende evaluaties zullen in voorkomend geval een dialoog over andere onderwerpen bevatten, zoals op het gebied van geautomatiseerde besluitvorming, met inbegrip van aspecten inzake de overeenkomsten en de verschillen in benadering tussen de EU en de VS.

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 privacyschild 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.

Uitzondering inzake de nationale veiligheid

Met betrekking tot de beperkingen op de naleving van de privacyschildbeginselen inzake de nationale veiligheid heeft de General Counsel van het bureau van de Director of National Intelligence, Robert Litt, ook twee brieven gestuurd aan Justin Antonipillai en Ted Dean van het ministerie van Handel, die ook aan u zijn doorgestuurd. In deze brieven worden onder andere uitvoerig het beleid, de waarborgen en de beperkingen besproken die van toepassing zijn op activiteiten van de VS op het gebied van signals intelligence. Daarnaast wordt in deze brieven de transparantie beschreven die de inlichtingendiensten over deze zaken bieden. Bij haar beoordeling van de privacyschildkaderregeling kan de Commissie aan de informatie uit deze brieven de zekerheid ontlenen om te kunnen concluderen dat het privacyschildregeling naar behoren, in overeenstemming met de daarin vervatte Beginselen, zal functioneren. Wij gaan ervan uit dat u bij de jaarlijkse evaluatie van de privacyschildkaderregeling in de toekomst, naast andere informatie, gebruik zult maken van de informatie die door de inlichtingendiensten openbaar is gemaakt.

Op grond van de Beginselen van het privacyschild en de begeleidende brieven en documenten, waaronder de toezeggingen van het ministerie inzake het beheer van en het toezicht op de privacyschildkaderregeling, verwachten wij dat de Commissie zal vaststellen dat de EU-VS-privacyschildkaderregeling voldoende 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 privacyschild zal worden voortgezet.

Met vriendelijke groet,

Ken Hyatt

Bijlage 2

Arbitrage-model

BIJLAGE I

Deze bijlage I beschrijft wanneer privacyschildorganisaties verplicht zijn klachten op grond van het Beginsel inzake 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-privacyschild vallen. Het doel van deze optie is een snel, onafhankelijk en eerlijk mechanisme te bieden, waarvan de betrokken personen desgewenst gebruik kunnen maken in geval van een geschil over schendingen van de Beginselen dat niet via een van de andere privacyschildmechanismen werden 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 privacyschildorganisatie 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 privacyschild.

B. **Beschikbare Rechtsmiddelen**

In het kader van deze arbitrage-optie is het privacyschildpanel (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, wissen of teruggave van de betrokken gegevens van de persoon) die nodig is om de schending van de Beginselen in verband met enkel deze persoon te verhelpen. Dit zijn de enige bevoegdheden van het arbitragepanel qua voorzieningen. Bij het overwegen van voorzieningen moet het arbitragepanel voorzieningen in overweging nemen die reeds door andere mechanismen werden vastgesteld in het kader van het privacyschild. Schadevergoeding of vergoeding van kosten of honoraria of andere voorzieningen zijn niet mogelijk. Elke partij betaalt de honoraria van zijn eigen advocaat.

C. **Aan abritrage voorafgaande vereisten**

Een 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 tegen de beweerde schending maken en de organisatie de gelegenheid bieden om de kwestie binnen de in sectie III, punt 11, onder (d) (i), van de Beginselen 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 betreffende gegevensbeschermingsautoriteit aankaarten bij het ministerie van Handel en dit ministerie de mogelijkheid bieden zijn uiterste best te doen om het probleem op de lossen binnen de termijnen die voorzien zijn in de Brief van de International Trade Administration van het ministerie van Handel. 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 betrokkene partij was; of 3) reeds eerder door de partijen werd geregeld. Bovendien kan deze optie niet worden ingeroepen als een EU-gegevensbeschermingsautoriteit 1) bevoegd is krachtens de secties III.5 of III.9 van de Beginselen, of 2) de bevoegdheid heeft om inzake de beweerde schending rechtstreeks met de organisatie tot een oplossing te komen. 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 persoon om deze bindende arbitrage-optie in te roepen is volledig vrijwillig. Arbitragebeslissingen zijn bindend voor alle partijen bij de arbitrage. Wanneer de betrokken persoon deze optie eenmaal heeft ingeroepen, doet hij afstand van de mogelijkheid om de zaak aan een andere forum voor te leggen, zij het dat wanneer de niet-geldelijke, billijke schadevergoeding de beweerde schending niet volledig vergoed, de keuze voor de arbitrage de betrokkene niet belet om eventueel bij de rechter een vordering tot schadevergoeding in te stellen.

([1]) Sectie I, punt 5, van de Beginselen.

E. **Rechterlijke toetsing en tenuitvoerlegging**

Particulieren en privacyschildorganisaties kunnen op grond van de Federal Arbitration Act de rechterlijke toetsing en tenuitvoerlegging van de arbitragebeslissingen vorderen krachtens Amerikaans recht ([1]). In dergelijke gevallen moet een zaak worden ingeleid bij het federal district court dat bevoegd is met betrekking tot de hoofdzetel van de privacyschild-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 rechtbanken in de EU of de VS, of FTC-procedures.

F. **Het arbitragepanel**

De partijen zullen de arbiters selecteren uit de hieronder besproken lijst van arbiters.

In overeenstemming met het toepasselijke recht zullen het ministerie van Handel van de Verenigde Staten en de Europese Commissie een lijst opstellen van ten minste 20 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 gedurende een periode van 3 jaar, behoudens buitengewone omstandigheden of dwingende redenen, welke periode met 3 jaar kan worden verlengd;

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

3) dienen toegelaten te zijn als advocaat in de Verenigde Staten en deskundige te zijn op het gebied van VS-wetgeving inzake privacybescherming, en deskundigheid te hebben op het gebied van EU-wetgeving inzake gegevensbescherming.

G. **Arbitrageprocedures**

In overeenstemming met het toepasselijke recht, moeten het ministerie van Handel en de Europese Commissie binnen zes maanden na de vaststelling van het adequaatheidsbesluit overeenstemming bereiken over de goedkeuring van een bestaande, beproefde reeks van VS-arbitrageprocedures (zoals AAA of JAMS) die worden toegepast op de procedures voor het privacyschildpanel, met inachtneming van de volgende onverwegingen:

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.

([1]) 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 transactie, overeenkomst of afspraak zoals beschreven in [sectie 2 van de FAA], valt onder het Verdrag [betreffende de erkenning en tenuitvoerlegging van buitenlandse scheidsrechterlijke uitspraken van 10 juni 1958, 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." *Id*. In hoofdstuk 2 wordt het volgende bepaald: „een partij bij de arbitrage mag een vordering instellen bij een rechtbank die bevoegd is op grond van dit hoofdstuk met het oog op een bevel tot bevestiging van de beslissing die werd genomen tegen een andere partij bij de arbitrage. De rechtbank zal de beslissing bevestigen tenzij zij meent dat er sprake is van een van de in genoemd Verdrag [van New York] vermelde redenen om de erkenning of de tenuitvoerlegging van de beslissing te weigeren of op te schorten." Id., § 207. Hoofdstuk 2 bepaalt voorts het volgende: „De districtscourts 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." Id. § 203.
In hoofdstuk 2 is ook bepaald dat „Hoofdstuk 1 […] van toepassing [is] 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." Id. § 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." *Id*. § 2. Hoofdstuk 1, bepaalt voorts dat „een partij bij de arbitrage mag deze rechtbank ook 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]." *Id*. § 9.

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 uitvoerende autoriteit mogen niet deelnemen aan deze arbitrages, zij het dat EU-gegevensbeschermingsautoriteiten op verzoek van een EU-burger 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 betrokken persoon door een advocaat wordt vertegenwoordigd, zal tijdens de arbitragezitting ten behoeve van de betrokken persoon voor kosteloze vertolking en kosteloze vertaling van de abitragestukken worden gezorgd, tenzij het panel 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 scheidsrechters worden voorgelegd, moeten vertrouwelijk behandeld worden 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 partijen anders overeengekomen is.

H. **Kosten**

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

In overeenstemming met het toepasselijke recht zal het ministerie van Handel de oprichting van een fonds bevorderen waaraan de privacyschildorganisaties 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 scheidsrechters, te dekken, ten belope van maximumbedragen („caps"), na overleg met de Europese Commissie. Het Fonds zal worden beheerd door een derde partij, die regelmatig verslag uitbrengt over de werkzaamheden van het Fonds. Bij de jaarlijkse evaluatie zullen het ministerie van Handel en de Europese Commissie de werking van het fonds evalueren, inclusief de vraag of het bedrag van de bijdragen of van de caps moet worden aangepast, en zullen zij onder andere het aantal arbitrages en de kosten en timing van de arbitrages in aanmerking nemen, waarbij er onderling van wordt uitgegaan dat aan de privacyschildorganisaties geen buitensporige financiële lasten zullen worden opgelegd. Honoraria voor advocaten vallen niet onder deze bepaling en worden ook niet gedekt door enig fonds uit hoofde van deze bepaling.

BIJLAGE II

BEGINSELEN INZAKE HET EU-VS-PRIVACYSCHILDKADER OPGESTELD DOOR HET AMERIKAANSE MINISTERIE VAN HANDEL

I. OVERZICHT

1. Terwijl de Verenigde Staten en de Europese Unie beide de privacybescherming willen verbeteren, benaderen de Verenigde Staten privacy anders dan de Europese Unie. De Verenigde Staten hebben een sectorale aanpak die is gebaseerd op een mix van wetgeving, regelgeving en zelfregulering. Gezien deze verschillen en teneinde organisaties in de Verenigde Staten een betrouwbaar mechanisme te bieden om persoonsgegevens vanuit de Europese Unie naar de Verenigde Staten door te geven, waarbij gewaarborgd wordt dat de betrokkenen in de EU blijven profiteren van effectieve waarborgen en bescherming zoals vereist door de Europese wetgeving ten aanzien van de verwerking van hun persoonsgegevens die zijn doorgegeven aan derde landen, heeft het ministerie van Handel deze Beginselen inzake het privacyschild opgesteld, met inbegrip van de aanvullende Beginselen (gezamenlijk „de Beginselen" genoemd) in het kader 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, het bedrijfsleven en andere belanghebbenden om de handel tussen de Verenigde Staten en de Europese Unie te bevorderen. Ze zijn uitsluitend bestemd voor gebruik door organisaties in de Verenigde Staten die persoonsgegevens uit de Europese Unie ontvangen om in aanmerking te kunnen komen voor het privacyschild en aldus te profiteren van het adequaatheidsbesluit van de Europese Commissie ([1]). De Beginselen hebben geen invloed op de toepassing van de nationale bepalingen ter uitvoering van Richtlijn 95/46/EG („de richtlijn") die van toepassing zijn op de verwerking van persoonsgegevens in de 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 privacyschild de doorgifte van persoonsgegevens uit de EU wordt geëffectueerd, moet een organisatie tegenover het ministerie van Handel (of de door deze aangewezen instantie) („het ministerie") verklaren dat zij door middel van zelfcertificering de Beginselen onderschrijft. Hoewel de beslissingen van organisaties om aldus deel te nemen aan het privacyschild 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 privacyschild moet een organisatie a) onderworpen zijn aan de onderzoeks- en handhavingsbevoegdheden van de Federal Trade Commission (de „FTC"), het ministerie van Vervoer of een andere officiële instantie die de effectieve naleving van de Beginselen zal waarborgen *(andere Amerikaanse officiële instanties 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. Wanneer een organisatie een en ander niet naleeft, kan handhavend worden opgetreden grond van artikel 5 van de Federal Trade Commission Act die oneerlijke en misleidende handelingen verbiedt op het gebied van of met invloed op de handel (15 U.S.C. § 45(a)) of op grond van andere wet- of regelgeving die dergelijke handelingen verbiedt.

3. Het ministerie van Handel 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 privacyschildlijst"). De voordelen van het privacyschild zijn gegarandeerd vanaf de datum dat het ministerie de organisatie op de privacyschildlijst plaatst. Het ministerie zal een organisatie van de privacyschildlijst verwijderen als zij zich vrijwillig terugtrekt uit het privacyschild of als ze nalaat haar jaarlijkse hercertificering bij het ministerie in te dienen. De verwijdering van een organisatie van de privacyschildlijst betekent dat zij niet langer kan profiteren van het adequaatheidsbesluit van de Europese Commissie om persoonsgegevens uit de EU te ontvangen. De organisatie moet de Beginselen blijven toepassen op de persoonsgegevens die zij heeft ontvangen toen zij aan het privacyschild deelnam, en elk jaar bij het ministerie opnieuw bevestigen dat zij dit zal blijven doen zolang zij dergelijke gegevens bewaart; anders moet de organisatie de gegevens teruggeven, verwijderen of „passende" bescherming van de informatie bieden met andere erkende middelen. Het ministerie zal ook de organisaties van de privacyschildlijst verwijderen die permanent nalaten om zich aan de Beginselen te houden; deze organisaties komen niet in aanmerking voor de privacyschildvoordelen en moeten de persoonsgegevens die zij op grond van het privacyschild hebben ontvangen, terugsturen of verwijderen.

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 zelfcertificeringsverklaring hadden ingediend, maar die van de privacyschildlijst zijn verwijderd. Het ministerie zal een duidelijke waarschuwing verstrekken dat deze organisaties geen deelnemer aan het privacyschild zijn, dat verwijdering van de privacyschildlijst betekent dat deze organisaties niet mogen beweren dat ze aan het privacyschild voldoen en zich moeten onthouden van alle verklaringen of misleidende praktijken waarmee wordt geïmpliceerd dat zij deelnemen aan het privacyschild, en dat dergelijke organisaties niet langer gerechtigd zijn om te profiteren van het adequaatheidsbesluit van de Europese

([1]) Op voorwaarde dat het besluit van de Commissie inzake het passend karakter van de door het EU-VS-privacyschild geboden bescherming van toepassing is op IJsland, Liechtenstein en Noorwegen, zal het privacyschild-pakket op zowel de Europese Unie 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.

Commissie dat die organisaties in staat zou stellen om persoonsgegevens uit de EU te ontvangen. Een organisatie die blijft beweren dat zij deelneemt aan het privacyschild of een andere aan het privacyschild gerelateerde verkeerde voorstellingen van zaken geeft nadat zij van de privacyschildlijst 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 om te voldoen aan vereisten inzake nationale veiligheid, het algemeen belang of rechtshandhaving; b) op grond van de wet, overheidsreglementering of jurisprudentie die tegenstrijdige verplichtingen of uitdrukkelijke bevoegdheden creëert, op voorwaarde dat een organisatie bij het uitoefenen van een dergelijke bevoegdheid kan aantonen dat haar niet-naleving van de Beginselen niet verder gaat dan nodig is om te voldoen aan de dwingende legitieme belangen die door een dergelijke bevoegdheid worden bevorderd; of c) indien met de richtlijn of de wetgeving van de lidstaat wordt beoogd uitzonderingen of afwijkingen toe te staan, mits deze uitzonderingen of afwijkingen in vergelijkbare situaties worden toegepast. In overeenstemming met het doel de privacybescherming te verbeteren, moeten organisaties ernaar streven om deze Beginselen volledig en op transparante wijze uit te voeren, en daarbij in hun privacybeleid vermelden in welke gevallen uitzonderingen op de Beginselen als toegestaan onder b) hierboven, regelmatig 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 om de Beginselen toe te passen op alle persoonsgegevens die op basis van het privacyschild zijn doorgegeven nadat zij zich voor het privacyschild hebben laten registreren. Een organisatie die ervoor kiest om de voordelen van het privacyschild 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 dient aan de in het aanvullende beginsel inzake zelfcertificering gestelde vereisten te voldoen.

7. De Amerikaanse wetgeving zal van toepassing zijn op kwesties inzake de interpretatie en naleving van de Beginselen en het relevante privacybeleid door de privacyschildorganisaties, behalve wanneer deze organisaties hebben toegezegd om samen te werken met de Europese 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 richtlijn vallen en door een organisatie in de Verenigde Staten vanuit de Europese Unie 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 middelen voor de verwerking van persoonsgegevens bepaalt.

9. De datum van inwerkingtreding van de Beginselen is de datum van de definitieve goedkeuring van het adequaatheidsbesluit van de Europese Commissie.

II. BEGINSELEN

1. **Kennisgeving**

   a) Een organisatie moet particulieren informeren over:

      i) haar deelname aan het privacyschild en een link verstrekken naar, of het webadres vermelden van, de privacyschildlijst,

      ii) de aard van de verzamelde persoonsgegevens en, indien van toepassing, de entiteiten of dochterondernemingen van de organisatie die de Beginselen ook onderschrijven,

iii) haar inzet om de Beginselen toe te passen op alle persoonsgegevens die in vertrouwen op het privacyschild vanuit Europa 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) het onafhankelijke orgaan voor geschillenbeslechting dat is aangewezen om klachten te behandelen en te voorzien in passende, kosteloze verhaalmogelijkheden voor de betrokken persoon, en of dat: 1) het panel is dat door gegevensbeschermingsautoriteiten is opgericht, 2) een alternatieve geschillenbeslechtingsinstantie is die in de EU gevestigd is, of 3) een alternatieve geschillenbeslechtingsinstantie 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,

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 veiligheid of rechtshandhaving, en

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

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

2. **Keuzemogelijkheden**

a) Een organisatie moet betrokkenen de mogelijkheid geven zich ertegen te verzetten (opt-out) dat hun persoonlijke informatie i) aan derden bekend zal worden gemaakt of ii) zal worden gebruikt voor een doel dat materieel verschilt van het (de) doel(en) waarvoor deze informatie oorspronkelijk is verzameld of waarvoor de betrokkene achteraf zijn toestemming heeft gegeven. Aan de betrokkene 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 betrokkene) moeten organisaties van de betrokkene positieve, expliciete toestemming (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 betrokkene 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 betrokkene 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 copie overleggen van de relevante privacybepalingen van de overeenkomst met die vertegenwoordiger.

4. **Beveiliging**

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 persoonlijke informatie.

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 verwerking ([1]). Een organisatie mag geen persoonlijke informatie verwerken op een wijze die onverenigbaar is met de doeleinden waarvoor deze is verzameld of waarmee de betrokkene 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 het individu slechts zolang identificeert of indentificeerbaar maakt ([2]) als dienstig is voor het doel van verwerking in de zin van punt 5, onder 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 kader van toepassing. Organisaties moeten redelijke en passende maatregelen nemen om aan deze bepaling te voldoen.

6. **Toegang**

a) Particulieren moeten toegang hebben tot de persoonlijke informatie die een organisatie over hen in bezit heeft, en 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 persoonlijke levenssfeer van de betrokkene, of de rechten van andere personen dan de betrokkene worden geschonden.

([1]) Al naargelang de omstandigheden kan het bij voorbeelden van compatibele 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 wettelijke rechten, of andere doeleinden die gelet op de context waarbinnen de informatie wordt verzameld, stroken met dat wat redelijkerwijs kan worden verwacht.

([2]) In dit verband is een individu „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, het individu redelijkerwijze kan worden geïdentificeerd door de organisatie of een derde partij indien die toegang tot de gegevens zou hebben.

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 consquenties 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 particulieren 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 verhaalmechanismen zullen onmiddellijk reageren op vragen en informatieverzoeken van het ministerie van Handel in verband met het privacyschild. 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.

c) Organisaties zijn verplicht klachten aan arbitrage te onderwerpen en de voorwaarden zoals uiteengezet in bijlage I na te leven, op voorwaarde dat de betrokkene door een kennisgeving aan 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 privacyschildorganisatie verantwoordelijk voor de verwerking van de persoonlijke informatie die zij ontvangt in het kader van het privacyschild en vervolgens doorgeeft aan een derde partij die in haar naam als vertegenwoordiger optreedt. De privacyschildorganisatie 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 jegens een organisatie een FTC- of een rechterlijke beslissing wordt genomen op grond van een niet-naleving, moet de organisatie alle relevante op het privacyschild betrekking hebbende passages in een bij de FTC ingediend nalevings-of beoordelingsverslag openbaar maken, voor zover dat strookt met de vereisten van vertrouwelijkheid. Het ministerie heeft een speciaal contactpunt voor gegevensbeschermingsautoriteiten opgericht voor problemen inzake naleving door privacyschildorganisaties. Het FTC zal 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 (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 betrokkene zelf openbaar zijn gemaakt.

2. **Uitzonderingen voor journalistieke doeleinden**

a) Gezien de in de grondwet van de Verenigde Staten neergelegde bescherming van de persvrijheid en de in de richtlijn neergelegde vrijstelling voor journalistiek materiaal 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 burgers 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 privacyschildbeginselen.

3. **Secundaire aansprakelijkheid**

a) Aanbieders van internetdiensten, telecommunicatiebedrijven of andere organisaties zijn niet aansprakelijk uit hoofde van de privacybeginselen wanneer zij namens een andere organisatie informatie enkel overbrengen, routeren, schakelen of opslaan. Evenmin als de richtlijn zelf voorziet het privacyschild in 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 betrokkene 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 privacyschildorganisaties, 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 privacyschildorganisatie 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 diligence, of accountants die een audit uitvoeren, mogen alleen informatie verwerken zonder dat de betrokkene 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 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 aankopen, 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 van de Europese Unie samen te werken zoals hieronder beschreven gestand doen. In het kader van het privacyschild zijn organisaties uit de Verenigde Staten die persoonsgegevens uit de Europese Unie ontvangen, verplicht effectieve mechanismen aan te wenden om de naleving van de privacyschildbeginselen 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 dergelijke 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 de samenwerking met de gegevensbeschermingsautoriteiten.

b) Een organisatie verplicht zich ertoe met de gegevensbeschermingsautoriteiten samen te werken door bij de indiening van haar zelfcertificering inzake het privacyschild bij het ministerie van Handel 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 privacyschildbeginsel 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 privacyschild 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 privacyschildbeginselen te voldoen, daaronder begrepen corrigerende en compenserende maatregelen ten gunste van 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 Europees panel van gegevensbeschermingsautoriteiten, 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 personen over de behandeling van persoonlijke informatie die vanuit de Europese Unie in het kader van het privacyschild is doorgegeven. Dit advies zal zo zijn opgesteld dat ervoor wordt gezorgd dat de privacyschildbeginselen correct worden toegepast en het zal de rechtsmiddelen voor de betrokkene (n) 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 personen ontvangen klachten tegen organisaties die zich ertoe verplicht hebben om in het kader van de privacyschilddoelstellingen 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 Federal Trade Commission, het ministerie van Vervoer of een andere instantie 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 van Handel hiervan op de hoogte brengen zodat de privacyschildlijst dienovereenkomstig kan worden gewijzigd. Elke niet-nakoming van de verplichting om met de gegevensbeschermingsautoriteiten samen te werken, alsmede elke niet-naleving van de privacyschildbeginselen kan op grond van sectie 5 van de FTC-wet of andere soortgelijke wetten als misleidende praktijk worden vervolgd.

d) Een organisatie die wil dat haar privacyschildbepalingen 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 deze mogelijkheid kiezen, betalen een jaarlijkse vergoeding ter dekking van de administratieve kosten van het panel. Wanneer het panel verwijzingen of klachten tegen de betrokken organisatie in overweging neemt, kan het bovendien een vergoeding van de kosten van eventueel noodzakelijke vertalingen verlangen. De jaarlijkse vergoeding bedraagt maximaal 500 USD, maar zal lager zijn voor kleinere ondernemingen.

6. **Zelfcertificering**

a) De voordelen van het privacyschild zijn gegarandeerd vanaf de datum waarop het ministerie op de privacyschildlijst heeft vermeld dat de zelfcertificering is ingediend, na te hebben geoordeeld dat de indiening volledig is.

b) Voor zelfcertificering in het kader van het privacyschild moet een organisatie bij het ministerie een zelfcertificering indienen, die door een directielid is ondertekend namens de organisatie die tot het privacyschild toetreedt en die ten minste de volgende informatie bevat:

i) naam van de organisatie, postadres, e-mailadres, telefoon-en fax;

ii) beschrijving van de activiteiten van de organisatie met betrekking tot de persoonslijke informatie die zij uit de EU ontvangt; en

iii) beschrijving van het 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;

2. de datum van inwerkingtreding;

3. een instantie waartoe men zich kan wenden voor de behandeling van klachten, verzoeken om toegang en alle andere kwesties die zich voordoen in het kader van het privacyschild;

4. 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 van de Beginselen of een toekomstige bijlage van de Beginselen);

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

6. de wijze van controle (bijv., intern, door derden) (zie het aanvullend Beginsel inzake verificatie); en

7. het onafhankelijk verhaalsmechanisme dat onopgeloste klachten kan onderzoeken.

c) Als een organisatie wil dat personeelsgegevens die vanuit de Europese Unie in het kader van een arbeidsverhouding zijn doorgegeven, eveneens onder de voordelen van het privacyschild vallen, kan zij dit bewerkstelligen indien een in de bijlage of toekomstige bijlage van 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 zelfcertificering 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.

d) Het ministerie zal een privacyschildlijst bijhouden van organisaties die volledige zelfcertificeringen hebben ingediend en zo in het genot komen van de voordelen van het privacyschild, en de lijst bijwerken aan de hand van jaarlijkse hercertificeringen en kennisgevingen die worden ontvangen ingevolge het aanvullend Beginsel inzake geschillenbeslechting en handhaving. Dergelijke zelfcertificeringen moeten minstens een keer per jaar worden ingediend; zo niet dan wordt de organisatie van de privacyschildlijst verwijderd en zijn de voordelen van het privacyschild niet langer gegarandeerd. Zowel de privacylijst als de door de organisaties ingediende zelfcertificeringen zullen voor het publiek toegankelijk worden gemaakt. Alle organisaties die door het ministerie op de privacyschildlijst zijn geplaatst, moeten in de verklaringen die zij publiceren over hun privacybeleid ook

aangeven dat zij de privacyschildbeginselen onderschrijven. In het privacybeleid van een organisatie moet, indien dat online beschikbaar is, een link staan naar de privacywebsite 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.

e) De privacybeginselen zijn onmiddellijk na de certificering van toepassing. Gelet op het feit dat de Beginselen invloed zullen hebben op de commerciële betrekkingen met derde partijen, moeten organisaties die door middel van certificering aan het privacyschildkader deelnemen in de eerste twee maanden na de datum van inwerkingtreding van het kader de bestaande commerciële relaties met derde partijen in overeenstemming brengen met het Beginsel van de aansprakelijkheid voor verdere doorgifte, en dat zo spoedig mogelijk en in elk geval uiterlijk negen maanden na de datum waarop zij door middel van certificering aan het privacyschild deelnemen. In die tussenliggende periode moeten organisaties wanneer zij gegevens aan een derde doorgeven i) het kennisbeginsel en het keuzebeginsel toepassen, en ii), wanneer persoonsgegevens worden doorgegeven aan een derde die als vertegenwoordiger optreedt, zich ervan vergewissen dat de vertegenwoordiger verplicht is ten minste hetzelfde beschermingsniveau te bieden als door de Beginselen wordt vereist.

f) Een organisatie moet op alle vanuit de EU op basis van het privacyschild ontvangen persoonsgegevens de privacyschildbeginselen toepassen. Voor persoonsgegevens die worden ontvangen tijdens de periode waarin de organisatie de voordelen van het privacyschild geniet, is de verplichting de privacyschildbeginselen 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 privacyschild deelneemt. Een organisatie die niet langer deelneemt aan het privacyschild, maar dergelijke gegevens wenst te behouden, moet jaarlijks aan het ministerie bevestigen dat zij zich ertoe verbindt de Beginselen te zullen blijven naleven of op een andere geautoriseerde wijze „passende" bescherming voor de informatie 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. Een organisatie die niet langer deelneemt aan het privacyschild moet waar relevant, in haar privacybeleid alle verwijzingen naar het privacyschild verwijderen die de indruk wekken dat ze nog steeds actief deelneemt aan privacyschild en recht heeft op de voordelen ervan.

g) Een organisatie die ten gevolge van een fusie of overname haar rechtspersoonlijkheid als zelfstandige onderneming zal verliezen, moet het ministerie hiervan vooraf in kennis stellen. In deze kennisgeving moet ook worden vermeld of de overnemende onderneming of de onderneming die door de fusie ontstaat i) op grond van de wetgeving die op de overname of fusie van toepassing is, nog steeds verplicht is zich aan de privacyschildbeginselen te houden of ii) verkiest de privacyschildbeginselen zelf te onderschrijven of andere garanties biedt, zoals een schriftelijke verklaring dat zij de privacyschildbeginselen zal naleven. Als noch i), noch ii) van toepassing is, moeten alle persoonsgegevens die in het kader van het privacyschild zijn verkregen, onmiddellijk worden verwijderd.

h) Wanneer een organisatie om welke reden dan ook niet langer aan het privacyschild deelneemt, moet zij alle verklaringen verwijderen waarmee wordt gesuggereerd dat zij aan het privacyschild blijft deelnemen of recht heeft op de voordelen ervan. Het EU-VS-privacyschildkeurmerk, indien gebruikt, moeten eveneens worden geschrapt. De FTC of een andere bevoegde overheidsinstantie kan actie ondernemen tegen iedere onjuiste verklaring aan het grote publiek met betrekking tot de naleving van de privacybeginselen 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. **Controle**

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 privacyschild afleggen, waar zijn en of dit beleid is uitgevoerd zoals het is voorgesteld en of het beantwoordt aan de privacyschildbeginselen.

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) Bij de zelfbeoordelingsmethode moet uit de controle blijken dat het gepubliceerde privacybeleid van een organisatie inzake uit de Europese Unie ontvangen persoonlijke informatie zorgvuldig en allesomvattend is, duidelijk wordt bekendgemaakt, volledig wordt uitgevoerd en toegankelijk is. Voorts moet blijken dat dit beleid in overeenstemming is met de privacyschildbeginselen, dat particulieren in kennis worden gesteld van interne regelingen voor de behandeling van klachten en van de onafhankelijke mechanismen om klachten in te dienen, dat de organisatie haar werknemers opleidt op het gebied van de uitvoering van het beleid en dat er disciplinaire maatregelen 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 controle van

de zelfbeoordeling moet minstens eens per jaar door een directielid of een andere daartoe bevoegde vertegenwoordiger van de organisatie worden ondertekend en op verzoek aan particulieren of in het kader van een onderzoek of een klacht wegens niet-naleving ter beschikking worden gesteld.

d) Indien de organisatie voor een externe controle van de naleving heeft gekozen, moet hieruit blijken dat het beleid inzake privacybescherming met betrekking tot uit de Europese Unie ontvangen persoonlijke informatie in overeenstemming is met de privacyschildbeginselen, dat het beleid wordt nageleefd en dat particulieren in kennis worden gesteld van de mechanismen om klachten in te dienen. 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 particulieren of in het kader van een onderzoek of een klacht wegens niet-naleving ter beschikking worden gesteld.

e) Organisaties moeten hun informatiebestanden over de tenuitvoerlegging van hun beleid inzake de bescherming van de privacy in het kader van het privacyschild bewaren en deze bij een onderzoek of een klacht wegens niet-naleving op verzoek ter beschikking stellen aan het onafhankelijke orgaan dat 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 privacyschildbeginselen 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 ([1]);

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) Particulieren behoeven een verzoek om toegang tot hun eigen gegevens niet te motiveren. Organisaties moeten zich bij hun reactie op een verzoek van een particulier 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 betrokkene 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 betrokkene 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, dient zij de betrokkene die om toegang verzoekt uit te leggen waarom zij tot dit besluit is gekomen en een contactadres op te geven waar de betrokkene met vragen terecht kan.

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 betrokkene 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 betrokkene. 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.

([1]) 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) Indien de persoonlijke informatie bijvoorbeeld gebruikt wordt voor beslissingen die voor de betrokkene 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 betrokkene 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.

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 betrokken persoon de betreffende persoonlijke informatie ter beschikking stelt en vereist niet dat de betrokken 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 richtlijn 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 betrokkenen de redenen voor het beperken van de toegang meedelen alsook een contactadres opgeven waar zij met verdere vragen terecht kunnen.

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

i) Een natuurlijk persoon heeft het recht om een bevestiging te verkrijgen of een organisatie al of niet persoonsgegevens over hem 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 betrokkene aanbiedt deze kosten te betalen.

g) Repetitieve of vexatoire verzoeken om toegang

Een organisatie kan het aantal keren dat binnen een bepaalde periode aan verzoeken van een bepaalde persoon gevolg wordt gegeven, binnen redelijke grenzen beperken. Bij het vaststellen van deze beperkingen moet een organisatie rekening houden met factoren als de frequentie waarmee de informatie wordt bijgewerkt, het doel waarvoor de gegevens worden gebruikt en de aard van de informatie.

h) Frauduleuze verzoeken om toegang

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

Op verzoeken om toegang moeten organisaties reageren binnen een redelijke termijn, op een redelijke wijze en in een vorm die voor de betrokken 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 privacyschild

i) Wanneer een organisatie in de EU persoonlijke informatie over zijn (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 privacyschild deelneemt, zijn de privacyschildbeginselen op deze doorgifte van toepassing. In deze gevallen was de nationale wetgeving van het EU-land waar de informatie werd verzameld, van toepassing op het verzamelen en verwerken van de doorgegeven informatie, zodat alle voorwaarden voor of restricties van de doorgifte die deze wetgeving stelt, in acht moeten worden genomen.

ii) De privacyschildbeginselen zijn alleen van toepassing wanneer bestanden over individueel bepaalde of bepaalbare 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 persoonlijke levenssfeer.

b) Toepassing van het kennisgevingsbeginsel en het keuzebeginsel

i) Een organisatie in de Verenigde Staten die in het kader van het privacyschild personeelsgegevens uit de Europese Unie heeft ontvangen, mag deze informatie alleen in overeenstemming met het kennisgevings-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 betrokkene achteraf heeft ingestemd. Bovendien mag hun keuze niet van invloed zijn op de carrièremogelijkheden van de werknemers 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 uitsluit, zelfs wanneer de informatie naar een land buiten de Europese Unie 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 kennis- en het keuzebeginsel niet toe te passen.

c) Toepassing van het toegangbeginsel

Het aanvullende toegangbeginsel 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 Europese Unie er overeenkomstig de wetgeving van hun land voor moeten zorgen dat hun werknemers in de Europese Unie toegang hebben tot dergelijke informatie, ongeacht de plaats waar de gegevens worden verwerkt en opgeslagen. Overeenkomstig de privacyschildbeginselen moet een organisatie die dergelijke gegevens in de Verenigde Staten verwerkt, deze toegang direct of via de werkgever in de Europese Unie 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 schending van de privacyschildbeginselen. 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 privacyschild deelnemende organisatie in de Verenigde Staten die gebruikmaakt van in het kader van een arbeidsverhouding vanuit de Europese Unie doorgegeven gegevens over personeel in de Europese Unie en die wil dat dergelijke doorgiften onder het privacyschild vallen, moet zich er dus toe verplichten mee te werken aan onderzoeken van de bevoegde autoriteiten in de Europese Unie en hun advies in dergelijke gevallen op te volgen.

e) Toepassing van het Beginsel van de aansprakelijkheid voor verdere doorgifte

Voor incidentele arbeidsgerelateerde operationele behoeften van de privacyschildorganisatie ten aanzien van in het kader van het privacyschild 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 privacyschildorganisatie 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 Europese Unie naar de Verenigde Staten worden doorgegeven, is een overeenkomst vereist, ongeacht of de verwerker aan het privacyschild deelneemt.

ii) De voor de verwerking verantwoordelijken in Europa moeten altijd een overeenkomst sluiten wanneer gegevens alleen voor verwerking worden doorgegeven, ongeacht of dit binnen de Europese Unie of daarbuiten gebeurt en ongeacht of de verwerker deelneemt aan het privacyschild. Het doel van de overeenkomst is ervoor te zorgen dat de verwerker:

1. slechts volgens 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 antwoorden van de personen die hun rechten uit hoofde van de Beginselen uitoefenen.

iii) Aangezien door de privacyschilddeelnemers passende bescherming wordt verleend, is er voor overeenkomsten met privacyschilddeelnemers die alleen de verwerking van gegevens ten doel hebben, geen voorafgaande toestemming nodig (of deze toestemming wordt automatisch door de EU-lidstaten verleend), hetgeen voor overeenkomsten met ontvangers die niet aan het privacyschild deelnemen of die geen passende bescherming bieden, wel vereist is.

b) Doorgifte binnen een gecontroleerde groep van ondernemingen of entiteiten

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. Voor de verwerking verantwoordelijken 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 controle programma's), waarmee de voortzetting van de bescherming van persoonlijke informatie in het kader van de privacyschildbeginselen wordt gegarandeerd. In geval van een dergelijke doorgifte blijft de privacyschild-organisatie verantwoordelijk voor de naleving van de privacyschildbeginselen.

c) Doorgifte tussen verwerkingsverantwoordelijken

Voor doorgifte tussen verwerkingsverantwoordelijken hoeft de ontvangende verwerkingsverantwoordelijke geen privacyschildorganisatie te zijn en niet te beschikken over een onafhankelijk verhaalsmechanisme. De privacyschildorganisatie moet een overeenkomst sluiten met de ontvangende derde verwerkingsverantwoordelijke, die dezelfde mate van bescherming biedt als beschikbaar is in het kader van het privacyschild, waarbij het niet vereist is dat de derde verwerkingsverantwoordelijke een privacyschildorganisatie is of beschikt over een onafhankelijke beroepsmechanisme, 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 privacyschild 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 privacyschildbeginselen 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 Europese Gemeenschap 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. Er zij op gewezen dat de eisen van het Beginsel van verhaal, handhaving en

aansprakelijkheid een aanvulling zijn op de eis dat bepalingen die het resultaat zijn van zelfregulering moeten kunnen worden gehandhaafd op grond van sectie 5 van de Federal Trade Commission Act, die oneerlijke en misleidende handelingen verbiedt, dan wel op grond van een andere wet of regeling die dergelijke handelingen verbiedt.

c) Om te bevorderen dat de nakoming van hun toezeggingen in het kader van het privacyschild wordt garandeerd en het beheer van het programma te ondersteunen, moeten de organisaties evenals hun onafhankelijke beroepsmechanismen informatie over het privacyschild 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 VS-wetgeving.

d) Verhaalsmechanismen

i) De consumenten moeten worden aangemoedigd eventuele klachten met de desbetreffende organisatie te bespreken alvorens een beroep te doen op onafhankelijke verhaalsmechanismen. Organisaties moeten een consument binnen 45 dagen na ontvangst van diens klacht een reactie doen toekomen. 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 particulieren direct beschikbaar en kosteloos zijn. Instanties die geschillen afhandelen, moeten alle klachten van particulieren onderzoeken tenzij deze duidelijk ongegrond of onbeduidend zijn. Dit sluit niet uit dat de organisatie 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 verhaalmechanismen particulieren 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 privacyschildbeginselen toegepaste praktijken inzake de privacybescherming. Zij moeten ook meewerken bij de ontwikkeling van hulpmiddelen als gestandaardiseerde klachtenformulieren om de klachtenafhandelingsprocedure te vergemakkelijken.

ii) Onafhankelijke verhaalsmechanismen moeten op hun openbare websites informatie opnemen over de privacyschildbeginselen en de diensten die zij in het kader van het privacyschild aanbieden. Deze informatie moet het volgende bevatten: 1) informatie over of een link naar de vereisten van privacyschildbeginselen voor onafhankelijke beroepsmechanismen; 2) een link naar de privacyschildwebsite van het ministerie; 3) een toelichting dat hun diensten inzake geschillenbeslechting in het kader van het privacyschild voor particulieren kosteloos zijn; 4) een beschrijving van de wijze waarop een klacht in verband met het privacyschild kan worden ingediend; 5) de termijnen waarbinnen klachten inzake het privacyschild worden behandeld; en 6) een beschrijving van de reeks van 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 het privacyschild; 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 particulieren over een arbitrage-optie teneinde ten aanzien van resterende klachten te bepalen of een privacyschildorganisatie 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. Zij 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 privacyschild. In het kader van deze arbitrage-optie is het privacyschildpanel (bestaande uit één of drie arbiters, zoals overeengekomen door de partijen) bevoegd om een individuele, specifieke, niet-geldelijke, billijke oplossing te gelasten (zoals toegang, correctie, schrapping of teruggave van de betrokken gegevens van de persoon) die nodig is om de schending van de Beginselen in verband met slechts deze persoon te verhelpen. Particulieren en privacyschildorganisaties kunnen op grond van de Federal Arbitration Act de rechterlijke toetsing en tenuitvoerlegging van de arbitragebeslissingen vorderen krachtens Amerikaans recht.

([1]) Sectie I, punt 5, van de Beginselen.

e) Rechtsmiddelen en sancties

De rechtsmiddelen die de geschillenafhandelingsinstantie 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 geschillenafhandelingsinstanties op passende wijze kunnen reageren op in ernst variërende gevallen van niet-naleving. Tot de sancties moeten behoren bekendmaking van geconstateerde gevallen van niet-naleving en de eis gegevens in bepaalde omstandigheden te wissen ([1]). 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 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 privacyschildorganisaties, en het ministerie daarvan op de hoogte stellen.

f) Actie van de FTC

De FTC zal prioriteit geven aan zaken die haar in verband met de niet-naleving van de Beginselen worden voorgelegd door: i) zelfregulerende organisaties 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 privacyschildbeginselen of deelname aan het privacyschild door organisaties die ofwel niet meer op de privacyschildlijst 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 hem van het uiteindelijke resultaat van dergelijke verwijzingen of andere uitspraken in verband met de naleving van de privacyschildbeginselen in kennis te stellen.

g) Permanente niet-naleving

i) Als een organisatie voortdurend de Beginselen overtreedt, komt ze niet langer in aanmerking voor de voordelen van het privacyschild. Een organisatie zal in geval van permanente niet-naleving van de privacybeginselen door het ministerie van de privacyschildlijst worden verwijderd en de in het kader van het privacyschild 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 constateert dat een organisatie zich vaak niet aan de Beginselen houdt en haar verklaring deze te zullen naleven niet langer geloofwaardig is. De organisatie moet het ministerie daarvan dan onverwijld 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 privacyschildlijst verwijderen wanneer zij ervan in kennis wordt gesteld dat een organisatie de Beginselen permanent niet naleeft, ongeacht of deze kennisgeving uitgaat van de organisatie zelf, van een zelfregulerende instantie op het gebied van de privacy of een ander zelfstandig geschillenbeslechtingsmechanisme, of van een overheidsinstantie, maar pas na de organisatie daarvan

([1]) 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 privacyschildbeginselen gegevens heeft verzameld of gebruikt, dan wel openbaar heeft gemaakt.

30 dagen van tevoren in kennis te hebben gesteld en de kans te hebben gegeven om te reageren. Uit deze door het ministerie bijgehouden privacyschildlijst blijkt derhalve welke organisaties verder voor de voordelen van het privacyschild in aanmerking komen en welke niet.

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

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

a) Het keuzebeginsel heeft ten 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 betrokkene. Daarom moet deze te allen tijde de mogelijkheid hebben zich tegen het gebruik van zijn persoonlijke informatie voor directe marketing te verzetten; hij dient dit wel te 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 persoon die zich verzet. In de Verenigde Staten kunnen particulieren dit recht uitoefenen via een centraal verzetprogramma zoals de Direct Marketing Association's Mail Preference Service. Organisaties die hieraan deelnemen, moeten de beschikbaarheid van deze dienst voor consumenten die geen commerciële informatie wensen te ontvangen, promoten. In ieder geval moet de betrokkene 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 betrokkene de gelegenheid te geven verzet aan te tekenen voordat de informatie wordt gebruikt, op voorwaarde dat de organisatie de betrokkene meteen daarna (en op verzoek altijd) de mogelijkheid biedt om verdere ontvangst van direct-marketingmededelingen te weigeren (zonder dat dit voor de consument kosten met zich brengt) en op voorwaarde dat de organisatie tegemoetkomt aan de wensen van de betrokkene.

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 Europese Unie worden doorgegeven. Ingevolge artikel 26 van de richtlijn mogen persoonsgegevens „naar een derde land dat geen waarborgen voor een passend beschermingsniveau in de zin van artikel 25, lid 2, biedt" worden doorgegeven op voorwaarde dat i) dit noodzakelijk is om de door de passagier gevraagde diensten te leveren of voor de uitvoering van de vervoersovereenkomst, zoals een bonusregeling; of ii) de passagier op ondubbelzinnige wijze met de doorgifte heeft ingestemd. Organisaties in de Verenigde Staten die aan het privacyschild deelnemen, zorgen voor een adequate bescherming van persoonsgegevens en kunnen daarom gegevens vanuit de Europese Unie ontvangen zonder te voldoen aan deze voorwaarden of aan andere in artikel 26 van de richtlijn genoemde voorwaarden. Aangezien het privacyschild specifieke regels voor gevoelige informatie omvat, kan dergelijke informatie (die soms moet worden verzameld, bijvoorbeeld omdat een passagier fysieke bijstand nodig heeft) naar deelnemers aan het privacyschild 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 privacyschildbeginselen

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 privacyschildbeginselen 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 privacyschild 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 het individu later toestemming heeft gegeven, is opnieuw toestemming vereist.

c) Opzegging van medewerking aan een klinische proef

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

Producenten van geneesmiddelen en medische apparatuur mogen persoonsgegevens uit in de Europese Unie 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 kennisgevings- 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

Producenten van geneesmiddelen en medische apparatuur hoeven de privacyschildbeginselen niet toe te passen met betrekking tot de Beginselen inzake 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

De hoofdonderzoeker voorziet de onderzoeksgegevens altijd al bij de bron van een unieke code, zodat de identiteit van de individuen 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 dusdanig gecodeerde gegevens van de EU naar de Verenigde Staten geldt niet als een doorgifte van persoonsgegevens waarop de privacyschildbeginselen van toepassing zijn.

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

a) Een organisatie moet de privacyschildbeginselen 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 restricties 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 privacyschild 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. Particulieren 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 privacyschildorganisaties op vrijwillige basis periodieke transparantieverslagen 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 privacyschildorganisaties in deze verslagen verstrekte informatie kan samen met de informatie die werd vrijgegeven door inlichtingendiensten, alsook andere informatie, gebruikt worden ten behoeve van de jaarlijkse gezamenlijke evaluatie van de werking van het privacyschild 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

Arbitrage-model

Deze bijlage I beschrijft wanneer privacyschildorganisaties verplicht zijn klachten op grond van het Beginsel inzake 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-privacyschild vallen. Het doel van deze optie is een snel, onafhankelijk en eerlijk mechanisme te bieden, waarvan de betrokken personen desgewenst gebruik kunnen maken in geval van een geschil over schendingen van de Beginselen dat niet via een van de andere privacyschildmechanismen werden 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 privacyschildorganisatie 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 privacyschild.

B. **Beschikbare rechtsmiddelen**

In het kader van deze arbitrage-optie is het privacyschildpanel (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, wissen of teruggave van de betrokken gegevens van de persoon) die nodig is om de schending van de Beginselen in verband met enkel deze persoon te verhelpen. Dit zijn de enige bevoegdheden van het arbitragepanel qua voorzieningen. Bij het overwegen van voorzieningen moet het arbitragepanel voorzieningen in overweging nemen die reeds door andere mechanismen werden vastgesteld in het kader van het privacyschild. Schadevergoeding of vergoeding van kosten of honoraria of andere voorzieningen zijn niet mogelijk. Elke partij betaalt de honoraria van zijn eigen advocaat.

C. **Aan abritrage voorafgaande vereisten**

Een 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 tegen de beweerde schending maken en de organisatie de gelegenheid bieden om de kwestie binnen de in sectie III, punt 11, onder (d) (i), van de Beginselen 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 betreffende gegevensbeschermingsautoriteit aankaarten bij het ministerie van Handel en dit ministerie de mogelijkheid bieden zijn uiterste best te doen om het probleem op de lossen binnen de termijnen die voorzien zijn in de Brief van de International Trade Administration van het ministerie van Handel. 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 betrokkenen partij was; of 3) reeds eerder door de partijen werd geregeld. Bovendien kan deze optie niet worden ingeroepen als een EU-gegevensbeschermingsautoriteit 1) bevoegd is krachtens de secties III.5 of III.9 van de Beginselen, of 2) de bevoegdheid heeft om inzake de beweerde schending rechtstreeks met de organisatie tot een oplossing te komen. 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 persoon om deze bindende arbitrage-optie in te roepen is volledig vrijwillig. Arbitragebeslissingen zijn bindend voor alle partijen bij de arbitrage. Wanneer de betrokken persoon deze optie eenmaal heeft ingeroepen, doet hij afstand van de mogelijkheid om de zaak aan een andere forum voor te leggen, zij het dat wanneer de niet-geldelijke, billijke schadevergoeding de beweerde schending niet volledig vergoed, de keuze voor de arbitrage de betrokkene niet belet om eventueel bij de rechter een vordering tot schadevergoeding in te stellen.

([1]) Sectie I, punt 5, van de Beginselen.

E. **Rechterlijke toetsing en tenuitvoerlegging**

Particulieren en privacyschildorganisaties kunnen op grond van de Federal Arbitration Act de rechterlijke toetsing en tenuitvoerlegging van de arbitragebeslissingen vorderen krachtens Amerikaans recht ([1]). In dergelijke gevallen moet een zaak worden ingeleid bij het federal district court dat bevoegd is met betrekking tot de hoofdzetel van de privacyschild-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 rechtbanken in de EU of de VS, of FTC-procedures.

F. **Het arbitragepanel**

De partijen zullen de arbiters selecteren uit de hieronder besproken lijst van arbiters.

In overeenstemming met het toepasselijke recht zullen het ministerie van Handel van de Verenigde Staten en de Europese Commissie een lijst opstellen van ten minste 20 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 gedurende een periode van 3 jaar, behoudens buitengewone omstandigheden of dwingende redenen, welke periode met 3 jaar kan worden verlengd;

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

3) dienen toegelaten te zijn als advocaat in de Verenigde Staten en deskundige te zijn op het gebied van VS-wetgeving inzake privacybescherming, en deskundigheid te hebben op het gebied van EU-wetgeving inzake gegevensbescherming.

G. **Arbitrageprocedures**

In overeenstemming met het toepasselijke recht, moeten het ministerie van Handel en de Europese Commissie binnen zes maanden na de vaststelling van het adequaatheidsbesluit overeenstemming bereiken over de goedkeuring van een bestaande, beproefde reeks van VS-arbitrageprocedures (zoals AAA of JAMS) die worden toegepast op de procedures voor het privacyschildpanel, met inachtneming van de volgende onverwegingen:

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.

([1]) 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 transactie, overeenkomst of afspraak zoals beschreven in [sectie 2 van de FAA], valt onder het Verdrag [betreffende de erkenning en tenuitvoerlegging van buitenlandse scheidsrechterlijke uitspraken van 10 juni 1958, 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." Id. In hoofdstuk 2 wordt het volgende bepaald: „een partij bij de arbitrage mag een vordering instellen bij een rechtbank die bevoegd is op grond van dit hoofdstuk met het oog op een bevel tot bevestiging van de beslissing die werd genomen tegen een andere partij bij de arbitrage. De rechtbank zal de beslissing bevestigen tenzij zij meent dat er sprake is van een van de in genoemd Verdrag [van New York] vermelde redenen om de erkenning of de tenuitvoerlegging van de beslissing te weigeren of op te schorten." Id. § 207. Hoofdstuk 2 bepaalt voorts het volgende: „De districtscourts 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." Id. § 203.
In Hoofdstuk 2 is ook bepaald dat „Hoofdstuk 1 […] van toepassing [is] 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." Id. § 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." Id. § 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]." Id. § 9.

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 uitvoerende autoriteit mogen niet deelnemen aan deze arbitrages, zij het dat EU-gegevensbeschermingsautoriteiten op verzoek van een EU-burger 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 betrokken persoon door een advocaat wordt vertegenwoordigd, zal tijdens de arbitragezitting ten behoeve van de betrokken persoon voor kosteloze vertolking en kosteloze vertaling van de abitragestukken worden gezorgd, tenzij het panel 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 scheidsrechters worden voorgelegd, moeten vertrouwelijk behandeld worden 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 moet worden voltooid binnen 90 dagen na de afgifte van de kennisgeving aan de betrokken organisatie, tenzij anders door partijen anders overeengekomen is.

H. **Kosten**

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

In overeenstemming met het toepasselijke recht zal het ministerie van Handel de oprichting van een fonds bevorderen waaraan de privacyschildorganisaties 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 scheidsrechters, te dekken, ten belope van maximumbedragen („caps"), na overleg met de Europese Commissie. Het Fonds zal worden beheerd door een derde partij, die regelmatig verslag uitbrengt over de werkzaamheden van het Fonds. Bij de jaarlijkse evaluatie zullen het ministerie van Handel en de Europese Commissie de werking van het fonds evalueren, inclusief de vraag of het bedrag van de bijdragen of van de caps moet worden aangepast, en zullen zij onder andere het aantal arbitrages en de kosten en timing van de arbitrages in aanmerking nemen, waarbij er onderling van wordt uitgegaan dat aan de privacyschildorganisaties geen buitensporige financiële lasten zullen worden opgelegd. Honoraria voor advocaten vallen niet onder deze bepaling en worden ook niet gedekt door enig fonds uit hoofde van deze bepaling.

BIJLAGE III

Brief van de Amerikaanse minister van Buitenlandse Zaken John Kerry

7 juli 2016

Geachte commissaris Jourová,

Ik ben blij dat wij overeenstemming hebben bereikt over het privacyschild tussen de Europese Unie — Verenigde Staten, dat een ombudsmanmechanisme zal bevatten door middel waarvan de autoriteiten in de EU verzoeken namens EU-burgers zullen kunnen indienen inzake praktijken in het kader van „inlichtingen uit berichtenverkeer" van de VS.

Op 17 januari 2014 heeft president Barack Obama belangrijke hervormingen van de inlichtingendienst aangekondigd, die zijn opgenomen in de Presidential Policy Directive 28 (Richtlijn Presidentieel Beleid — PPD-28). Krachtens PPD-28 heb ik Under Secretary of State Catherine A. Novelli, tevens belast met de functie van Senior Coordinator for International Information Technology Diplomacy, aangewezen als ons contactpunt voor buitenlandse regeringen die zaken aan te orde wensen te stellen in verband met activiteiten van de VS met betrekking tot inlichtingen uit het berichtenverkeer. Voortbouwend op deze taak heb ik een privacyschildombudsman-mechanisme ingesteld overeenkomstig de in bijlage A uiteengezette voorwaarden, welke sinds mijn brief van 22 februari 2016 zijn geactualiseerd. Ik heb Under Secretary Novelli met deze functie belast. Under Secretary Novelli is onafhankelijk van de VS inlichtingendiensten en brengt rechtstreeks verslag aan mij uit.

Ik heb mijn ambtenaren de opdracht gegeven de nodige middelen ter beschikking te stellen voor de uitvoering van dit nieuwe ombudsmanmechanisme en ik heb er alle vertrouwen in dat het een doeltreffend middel zal zijn om zorgen van EU-burgers weg te nemen.

Met vriendelijke groet,

John F. Kerry

Bijlage A

EU-VS-privacyschildombudsmanmechanisme met betrekking tot inlichtingen uit het berichtenverkeer

Gelet op het belang van het EU-VS-privacyschildkader bevat dit Memorandum de procedure voor de uitvoering van een nieuw mechanisme, in overeenstemming met de Presidential Policy Directive 28 (PPD-28), met betrekking tot inlichtingen uit het berichtenverkeer ([1]).

Op 17 januari 2014 heeft president Obama een toespraak gehouden waarin belangrijke hervormingen van de inlichtingendienst werd aangekondigd. In deze toespraak, wees hij erop dat „[o]nze inspanningen […] niet alleen [bijdragen] tot de bescherming van ons land, maar ook van onze bondgenoten en vrienden. Onze inspanningen zullen pas effectief zijn als normale burgers in andere landen erop vertrouwen dat ook de Verenigde Staten hun persoonlijke levenssfeer respecteren." president Obama kondigde de uitvaardiging aan van een nieuwe presidentiële richtlijn — PPD-28 — teneinde „duidelijk te bepalen wat we doen, en niet doen, als het op onze overzeese observatie aankomt."

Sectie 4(d) van 28-PPD geeft de minister van Buitenlandse Zaken de opdracht om een „Senior Coordinator for International Information Technology Diplomacy" (Senior Coordinator) te benoeme, die moet „te dienen als aanspreekpunt voor buitenlandse regeringen die bezorgd zijn over activiteiten van de Verenigde Staten met betrekking tot inlichtingen uit berichtenverkeer." Met ingang van januari 2015 is C. Novelli de Senior Coördinator.

Dit memorandum beschrijft een nieuw mechanisme dat de Senior Coordinator zal toepassen om eenvoudiger verzoeken te kunnen behandelen met betrekking tot de toegang in verband met de nationale veiligheid tot gegevens die vanuit de EU zijn doorgegeven naar de Verenigde Staten in het kader van het privacyschild, modelcontractbepalingen, bindende bedrijfsvoorschriften, „afwijkingen" ([2]) of „mogelijke toekomstige afwijkingen" ([3]), via gevestigde kanalen uit hoofde van toepasselijke VS-wetgeving en -beleidregels, en het antwoord op die verzoeken.

1. **De privacyschildombudsman.** De Senior Coördinator fungeert als privacyschildombudsman en wijst ambtenaren van het ministerie van Buitenlandse Zaken aan om haar zo nodig bij te staan in de uitoefening van de in dit memorandum omschreven verantwoordelijkheden. (Hierna zullen de Coördinator en de ambtenaren die dergelijke taken verrichten worden aangeduid als „privacyschildombudsman".) De privacyschildombudsman zal nauw samenwerken met de daarvoor in aanmerking komende ambtenaren van andere ministeries en agentschappen die verantwoordelijk zijn voor de verwerking van verzoeken overeenkomstig de toepasselijke wetten en beleidsregels van de Verenigde Staten. De ombudsman is onafhankelijk van de inlichtingendiensten. De ombudsman brengt rechtstreeks verslag uit aan de minister van Buitenlandse Zaken, die ervoor zal zorgen dat de ombudsman zijn taak uitoefent op objectieve wijze en vrij van ongepaste beïnvloeding die gevolgen voor het te geven antwoord kan hebben.

2. **Doeltreffende coördinatie.** De privacyschildombudsman zal effectief gebruik kunnen maken en tot afstemming kunnen komen met de hieronder beschreven toezichthoudende organen, teneinde ervoor te zorgen dat het antwoord van de ombudsman op de vragen die worden ingediend door de EU-instantie voor de behandeling van individuele

([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 privacyschild-pakket op zowel de Europese Unie 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]) In deze context wordt onder „Afwijkingen" verstaan: een commerciële doorgifte of commerciële doorgiften die plaatsvinden op voorwaarde dat: a) de betrokkene ondubbelzinnig toestemming voor de voorgestelde doorgifte heeft gegeven; of b) de doorgifte noodzakelijk is voor de uitvoering van een overeenkomst tussen de betrokkene en de verantwoordelijke voor de verwerking of voor de uitvoering van op verzoek van de betrokkene genomen precontractuele maatregelen; of c) de doorgifte noodzakelijk is voor de sluiting of de uitvoering van een in het belang van de betrokkene gesloten overeenkomst tussen de verantwoordelijke voor de verwerking en een derde; of d) de doorgifte noodzakelijk of wettelijk verplicht is vanwege een zwaarwegend algemeen belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte; of e) de doorgifte noodzakelijk is ter vrijwaring van het vitale belang van de betrokkene; of f) de doorgifte geschiedt vanuit een openbaar register dat krachtens wettelijke of bestuursrechtelijke bepalingen bedoeld is om het publiek voor te lichten en dat door een ieder dan wel door iedere persoon die zich op een gerechtvaardigd belang kan beroepen, kan worden geraadpleegd, voor zover in het betrokken geval is voldaan aan de wettelijke voorwaarden voor raadpleging.

([3]) Onder „Mogelijk Toekomstig Afwijkingen" wordt in deze context verstaan: een commerciële doorgifte of commerciële doorgiften die plaatsvind(t)(en) onder één van de volgende voorwaarden, voor zover de voorwaarde een gerechtvaardigde reden vormt voor doorgifte van persoonsgegevens van de EU naar de VS: a) de betrokkene heeft uitdrukkelijk met de voorgestelde doorgifte ingestemd, na te zijn ingelicht over de risico's die dergelijke doorgiften voor hem kunnen inhouden bij ontstentenis van een adequaatheidsbesluit en van passende waarborgen; of b) de doorgifte is noodzakelijk voor de bescherming van de vitale belangen van de betrokkene of van andere personen, indien de betrokkene lichamelijk of juridisch niet in staat is zijn toestemming te geven; of c) in geval van een doorgifte naar een derde land of een internationale organisatie alleen indien de doorgifte niet repetitief is, alleen betrekking heeft op een beperkt aantal betrokkenen, noodzakelijk is voor de zwaarwegende gerechtvaardigde belangen van de verwerkingsverantwoordelijke die niet worden opgeheven door de belangen of de rechten en vrijheden van de betrokkene, en de verwerkingsverantwoordelijke alle omstandigheden inzake de doorgifte heeft beoordeeld en op basis van deze beoordeling passende waarborgen heeft geboden voor de bescherming van persoonsgegevens.

klachten gebaseerd is op de noodzakelijke informatie. Wanneer het verzoek betrekking heeft op de verenigbaarheid van surveillance met de wetgeving van de VS zal de ombudsman kunnen samenwerken met een van de onafhankelijke toezichthoudende organen met onderzoeksbevoegdheden.

a) De privacyschildombudsman zal nauw samenwerken met andere regeringsambtenaren van de Verenigde Staten, waaronder passende daarvoor in aanmerking komende toezichthoudende organen, om ervoor te zorgen dat verzoeken volledig zijn en in overeenstemming met de toepasselijke wetten en beleidsregels worden behandeld en afgehandeld. In het bijzonder zal de privacyschildombudsman nauw kunnen samenwerken met het bureau van de directeur van de nationale inlichtingendienst, het ministerie van Justitie en andere ministeries en agentschappen die in voorkomend geval betrokken zijn bij de nationale veiligheid van de Verenigde Staten, en met inspecteurs-generaal, ambtenaren die met de uitvoering van de Freedom of Information Act zijn belast en ambtenaren op het gebied van burgerlijke vrijheden en privacy.

b) De regering van de Verenigde Staten zal gebruikmaken van ministeries en agentschappen overkoepelende mechanismen voor de coördinatie van en toezicht op aangelegenheden van nationale veiligheid, om ervoor te zorgen dat de privacyschildombudsman in staat is te reageren in de zin van sectie 4(e) op volledige verzoeken krachtens sectie 3(b).

c) De privacyschildombudsman kan aangelegenheden in verband met verzoeken ter overweging doorverwijzen naar de Privacy and Civil Liberties Oversight Board.

3. **Indiening van verzoeken.**

a) Een verzoek wordt in eerste instantie ingediend bij de toezichthoudende autoriteiten in de lidstaten die bevoegd zijn voor het toezicht op de nationale veiligheidsdiensten en/of de verwerking van persoonsgegevens door overheidsdiensten. Het verzoek wordt ingediend bij de ombudsman door een centraal EU-orgaan (hierna de „EU-instantie voor de behandeling van individuele klachten" genoemd).

b) De EU-instantie voor de behandeling van individuele klachten zal er, door middel van de volgende handelingen, op toezien dat het verzoek volledig is:

i) door de identiteit van de persoon te controleren en door te controleren of de persoon in eigen naam handelt en niet als vertegenwoordiger van een gouvernementele of een intergouvernementele organisatie;

ii) door erop toe te zien dat het verzoek schriftelijk wordt ingediend en dat het de volgende basisinformatie bevat:

— alle informatie die de basis vormt voor het verzoek,

— de aard van de informatie of het gewenste herstel,

— in voorkomend geval de nationale overheidsorganen van de Verenigde Staten die geacht worden betrokken te zijn, en

— de andere maatregelen die zijn genomen om de gevraagde informatie of het gevraagde herstel te verkrijgen en het naar aanleiding van die andere maatregelen ontvangen antwoord;

iii) door te controleren of het verzoek betrekking heeft op gegevens die redelijkerwijs worden verondersteld uit de EU te zijn doorgegeven naar de Verenigde Staten in het kader van het privacyschild, modelcontractbepalingen, bindende bedrijfsvoorschriften, afwijkingen, of mogelijke toekomstige afwijkingen;

iv) door het doen van een eerste vaststelling dat het verzoek niet lichtzinnig, vexatoir, of te kwader trouw werd gedaan.

c) Om met het oog op een verdere behandeling door de privacyschildombudsman in het kader van dit memorandum volledig te zijn, hoeft in het verzoek niet te worden aangetoond dat de regering van de Verenigde Staten via activiteiten in het kader van inlichtingen uit het berichtenverkeer feitelijk toegang heeft gehad tot de gegevens van de verzoeker.

4. **Toezeggingen om met de indienende EU-instantie voor de behandeling van individuele klachten te communiceren.**

a) De privacyschildombudsman bevestigt de ontvangst van het verzoek aan de indienende EU-instantie voor de behandeling van individuele klachten.

b) De privacyschildombudsman voert een eerste onderzoek uit om te controleren of het verzoek volledig is in de zin van sectie 3(b). Indien de privacyschildombudsman gebreken constateert of vragen heeft over de volledigheid van het verzoek, dan tracht de ombudsman deze kwesties samen met de indienende EU-instantie voor de behandeling van individuele klachten aan te pakken en op te lossen.

c) Indien de privacyschildombudsman voor de juiste verwerking van het verzoek meer informatie nodig heeft over het verzoek of als specifieke actie moet worden ondernomen door de persoon die het verzoek oorspronkelijk heeft ingediend, dan informeert de privacyschildombudsman de indienende EU-instantie voor de behandeling van individuele klachten daarover.

d) De privacyschildombudsman volgt de stand van zaken van de behandeling van de verzoeken en verstrekt zo nodig updates aan de indienende EU-instantie voor de behandeling van individuele klachten.

e) Wanneer een verzoek volledig is in de zin van sectie 3 van dit memorandum stuurt de privacyschildombudsman tijdig een passend antwoord aan de indienende EU-instantie voor de behandeling van individuele klachten, onder de voortdurende verplichting informatie te beschermen op grond van toepasselijke wetgeving en beleidsregels. De privacyschildombudsman stuurt een antwoord aan de indienende EU-instantie voor de behandeling van individuele klachten waarin wordt bevestigd i) dat de klacht naar behoren is onderzocht en ii) dat is voldaan aan de wetgeving van de VS, uitvoeringsbevelen, presidentiële richtlijnen en beleidsmaatregelen van instanties die voorzien in de beperkingen en waarborgen die worden beschreven in de ODNI-brief, of, indien er sprake is van niet-naleving, dat deze niet-naleving is verholpen. De privacyschildombudsman zal bevestigen noch ontkennen dat de betrokkene het voorwerp is geweest van surveillance, noch zal de privacyschildombudsman de specifieke oplossing bevestigen die werd gekozen. Zoals nader toegelicht in sectie 5 worden verzoeken in het kader van de Freedom of Information Act verwerkt zoals bepaald in die wet en in de toepasselijke verordeningen.

f) De privacyschildombudsman onderhoudt rechtstreeks contact met de EU-instantie voor de behandeling van individuele klachten, die vervolgens verantwoordelijk is voor de communicatie met de betrokkene die het verzoek indient. Indien rechtstreekse contacten onderdeel uitmaken van een van de hierna beschreven onderliggende processen, dan vinden deze contacten plaats in overeenstemming met de bestaande procedures.

g) De toezeggingen in dit memorandum zijn niet van toepassing op algemene beweringen dat het EU-VS-privacyschild inconsistent is met de vereisten van de Europese Unie op het gebied van gegevensbescherming. De toezeggingen in dit memorandum zijn gedaan op basis van de consensus tussen de Europese Commissie en de regering van de VS dat er, gezien de reikwijdte van de toezeggingen op grond van dit mechanisme, budgettaire beperkingen kunnen ontstaan, onder meer met betrekking tot verzoeken op grond van de Freedom of Information Act. Mocht de uitoefening van de privacyschildombudsfunctie de redelijke beperkingen van de middelen overschrijden en de naleving van deze toezeggingen belemmeren, dan zal de regering van de VS met de Europese Commissie eventuele aanpassingen bespreken die nodig kunnen zijn om deze situatie aan te pakken.

5. **Verzoeken om informatie.** Verzoeken om toegang tot gegevens van de Amerikaanse overheid kunnen op grond van de Freedom of Information Act (FOIA) worden ingediend en verwerkt.

a) De FOIA biedt eenieder die toegang wil krijgen tot bestaande gegevens van een federale instantie de mogelijkheid deze toegang te krijgen, ongeacht de nationaliteit van de verzoeker. Deze wet is in de United States Code vastgelegd in 5 U.S.C. § 552. Deze wet is, samen met aanvullende informatie over de FOIA, beschikbaar op www.FOIA.gov en http://www.justice.gov/oip/foia-resources. Elke instantie heeft een functionaris die hoofdverantwoordelijk is voor kwesties aangaande de FOIA en heeft op zijn openbare website informatie verstrekt over de wijze waarop een verzoek op grond van deze wet kan worden ingediend bij de instantie. Instanties hebben procedures ingesteld voor het raadplegen van andere instanties in het kader van verzoeken op grond van de FOIA Act die betrekking hebben op gegevens die door andere instanties worden bewaard.

b) Een voorbeeld:

i) Het bureau van de directeur van de nationale inlichtingendienst (ODNI) heeft een specifiek portaal ingesteld met betrekking tot de FOIA en het ODNI: http://www.dni.gov/index.php/about-this-site/foia. Dit portaal verstrekt informatie over het indienen van een verzoek, het controleren van de stand van zaken met betrekking tot een reeds ingediend verzoek en het verkrijgen van toegang tot informatie die door het bureau is vrijgegeven en openbaar gemaakt op grond van de FOIA. Het ODNI-FOIA-portaal bevat tevens links naar andere websites in het kader van de FOIA voor onderdelen van de inlichtingendiensten: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

ii) Het bureau voor informatiebeleid van het Amerikaanse ministerie van Justitie biedt uitgebreide informatie over de FOIA: http://www.justice.gov/oip. Daarbij gaat het niet alleen om informatie over het indienen van een verzoek op grond van de FOIA bij het ministerie van Justitie, maar ook om richtsnoeren voor de Amerikaanse overheid over de interpretatie en toepassing van vereisten in het kader van de FOIA.

c) Op grond van de FOIA is de toegang tot gegevens van de regering onderworpen aan bepaalde, één voor één genoemde uitzonderingen. Het betreft onder meer beperkingen van de toegang tot vertrouwelijke informatie over de nationale veiligheid, persoonlijke informatie van derden en informatie met betrekking tot onderzoeken in het kader van de rechtshandhaving, welke vergelijkbaar zijn met de beperkingen die elke EU-lidstaat oplegt op grond van de eigen wetgeving inzake de toegang tot informatie. Deze beperkingen gelden zowel voor Amerikanen als niet-Amerikanen.

d) In geschillen met betrekking tot de vrijgave van gegevens waarom op grond van de FOIA is verzocht, kan administratief beroep en vervolgens beroep bij de federale rechter worden ingesteld. De rechtbank moet opnieuw beoordelen of de gegevens terecht niet zijn vrijgegeven, 5 U.S.C. § 552(a)(4)(B), en kan de regering dwingen toegang tot de gegevens te verlenen. De rechtbank heeft in sommige gevallen geoordeeld dat de verklaring van de overheid dat informatie vanwege de vertrouwelijkheid niet mocht worden vrijgegeven, onterecht was. Hoewel er geen geldelijke compensatie kan worden toegekend, kan de rechtbank wel een vergoeding van de honoraria van advocaten toekennen.

6. **Verzoeken om verdere actie.** Een verzoek waarin sprake is van vermeende schending van het recht of ander wangedrag wordt doorgeleid naar de bevoegde instantie van de Amerikaanse overheid, waaronder onafhankelijke toezichtsinstanties, die bevoegd is om het desbetreffende verzoek te onderzoeken en niet-naleving aan te pakken zoals hieronder beschreven.

a) Een inspecteur-generaal is wettelijk onafhankelijk, heeft een ruime bevoegdheid om onderzoek, audits en evaluaties van programma's uit te voeren, onder meer op het gebied van fraude en misbruik of schending van de wet, en kan corrigerende maatregelen voorstellen.

i) Op grond van de Inspector General Act van 1978, zoals gewijzigd, fungeren binnen de meeste instanties federale inspecteurs-generaal (IG) als onafhankelijke en objectieve eenheden met als taak de bestrijding van verspilling, fraude en misbruik binnen de programma's en operaties van hun respectieve instanties. Elke IG is daartoe verantwoordelijk voor het uitvoeren van audits en onderzoeken met betrekking tot de programma's en operaties van zijn instantie. Daarnaast bieden de IG's leiding en coördinatie en geven ze beleidsaanbevelingen voor activiteiten ter bevordering van besparingen, efficiëntie en doeltreffendheid en ter voorkoming en opsporing van fraude en misbruik in het kader van programma's en operaties van de instantie.

ii) Elk onderdeel van de inlichtingendiensten heeft zijn eigen bureau van de inspecteur-generaal dat verantwoordelijk is voor, onder andere, het toezicht op de buitenlandse inlichtingenactiviteiten. Een aantal rapporten van inspecteurs-generaal over inlichtingenprogramma's zijn openbaar gemaakt.

iii) Een voorbeeld:

— Het bureau van de inspecteur-generaal van de inlichtingendiensten (IC IG) is opgericht op grond van artikel 405 van de Intelligence Authorization Act of Fiscal Year 2010. Het IC IG is verantwoordelijk voor het uitvoeren van zich over alle inlichtingendiensten uitstrekkende audits, onderzoeken, inspecties en evaluaties waarbij systeemrisico's, kwetsbaarheden en tekortkomingen worden vastgesteld en aangepakt die de afzonderlijke instanties van de inlichtingendiensten overstijgen, teneinde op positieve wijze bij te dragen tot besparingen en doelmatigheid binnen de inlichtingendiensten in hun geheel. Het IC IG heeft de bevoegdheid om klachten of informatie te onderzoeken met betrekking tot een schending van het recht of van een regel of regeling, verspilling, fraude, misbruik van gezag of een aanzienlijk of specifiek gevaar voor de volksgezondheid en de openbare veiligheid in verband met de inlichtingenprogramma's en -activiteiten van het ODNI en/of de inlichtingendiensten. Het IC IG verstrekt informatie over de wijze waarop rechtstreeks contact kan worden opgenomen met het IC IG voor het indienen van een rapport: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

— Het bureau van de inspecteur-generaal (OIG) binnen het Amerikaanse ministerie van Justitie (DOJ) is een bij wet opgerichte onafhankelijke entiteit met als missie de opsporing en bestrijding van verspilling, fraude, misbruik en wangedrag binnen DOJ-programma's en bij DOJ-personeel, en de bevordering van besparingen en doelmatigheid bij deze programma's. Het OIG onderzoekt vermeende schendingen van strafrecht en civiel recht door DOJ-werknemers en voert tevens audits en inspecties uit inzake DOJ-programma's. Het OIG heeft rechtsbevoegdheid ten aanzien van alle klachten over wangedrag tegen werknemers van het DOJ, waaronder het Federal Bureau of Investigation, de Drug Enforcement Administration, het Federal Bureau of Prisons, de U.S. Marshals Service, het Bureau of Alcohol, Tobacco, Firearms, and Explosives, de United States Attorneys Offices, en werknemers die werkzaam zijn in andere afdelingen of bureaus van het ministerie van Justitie. (De enige uitzondering hierop is dat beschuldigingen van wangedrag van een advocaat of wetshandhavend personeel van het ministerie dat verband houdt met de uitoefening van de bevoegdheid van de advocaat van het ministerie om te onderzoeken, procederen of

juridisch advies te verstrekken, onder de verantwoordelijkheid vallen van het bureau voor Office of Professional Responsibility van het ministerie.) Daarnaast belast sectie 1001 van de USA Patriot Act, die in werking is getreden op 26 oktober 2001, de inspecteur-generaal met de taak om informatie te evalueren en klachten te behandelen inzake vermeend misbruik van burgerrechten en burgerlijke vrijheden door werknemers van het ministerie van Justitie. Het OIG beschikt over een openbare website, https://www.oig.justice.gov, waar tevens een „hotline" te vinden is voor het indienen van klachten: https://www.oig.justice.gov/hotline/index.htm.

b) Bureaus en entiteiten van de Amerikaanse overheid op het gebied van privacy en burgerlijke vrijheden hebben ook relevante verantwoordelijkheden. Een voorbeeld:

i) In sectie 803 van de uitvoeringsaanbevelingen inzake de 9/11 Commission Act van 2007, gecodificeerd in de United States Code onder 42 U.S.C.§ 2000-ee1, worden bij bepaalde ministeries en instanties (waaronder de ministeries van Buitenlandse Zaken en van Justitie en het ODNI) functionarissen voor privacy en burgerlijke vrijheden aangesteld. In sectie 803 wordt bepaald dat deze functionarissen voor privacy en burgerlijke vrijheden fungeren als voornaamste adviseur om er, onder andere, voor te zorgen dat het ministerie, de instantie of het onderdeel in kwestie over passende procedures beschikt om klachten te behandelen van betrokkenen die stellen dat het ministerie, de instantie of het onderdeel hun privacy of burgerlijke vrijheden heeft geschonden.

ii) Het bureau voor burgerlijke vrijheden en privacy van het ODNI (ODNI-CLPO) wordt geleid door de functionaris voor de bescherming van burgerlijke vrijheden van het ODNI, een functie die is ingevoerd bij de National Security Act van 1948, zoals gewijzigd. De taken van het ODNI-CLPO bestaan er onder meer in te verzekeren dat het beleid en de procedures van de onderdelen van de inlichtingendiensten de privacy en burgerlijke vrijheden voldoende bescherming bieden en klachten te beoordelen en onderzoeken waarin wordt gesteld dat er misbruik of schending van burgerlijke vrijheden en privacy heeft plaatsgevonden in het kader van programma's en activiteiten van het ODNI. Het ODNI-CLPO verstrekt informatie aan het publiek op zijn website, waaronder instructies over de wijze waarop een klacht kan worden ingediend: www.dni.gov/clpo. Als het ODNI-CLPO een klacht over privacy of burgerlijke vrijheden ontvangt met betrekking tot programma's en activiteiten van de inlichtingendiensten, coördineert het bureau met andere onderdelen van de inlichtingendiensten de wijze waarop die klacht binnen de inlichtingendiensten verder moet worden afgehandeld. Opgemerkt zij dat het National Security Agency (NSA) ook een bureau voor burgerlijke vrijheden en privacy heeft, dat informatie over zijn verantwoordelijkheden verstrekt op zijn website: https://www.nsa.gov/civil_liberties/. Voor het geval uit informatie blijkt dat een instantie de privacyvereisten niet naleeft (bijvoorbeeld een vereiste op grond van sectie 4 van PPD-28), beschikken instanties over nalevingsmechanismen om het incident te beoordelen en een oplossing te bieden. Instanties zijn op grond van PPD-28 verplicht om nalevingsincidenten te melden bij het ODNI.

iii) Het bureau voor privacy en burgerlijke vrijheden (OPCL) binnen het ministerie van Justitie ondersteunt de taken en verantwoordelijkheden van de hoofdfunctionaris voor privacy en burgerlijke vrijheden (CPCLO) van het ministerie. De voornaamste taak van de OPCL is het beschermen van de privacy en burgerlijke vrijheden van het Amerikaanse volk door middel van evaluatie, toezicht en coördinatie inzake de activiteiten van het ministerie op het gebied van privacy. Het OPCL verstrekt juridisch advies en richtsnoeren aan onderdelen van het ministerie, verzekert dat het ministerie de privacyvereisten naleeft, waaronder de vereisten van de Privacy Act van 1974 en de privacybepalingen van zowel de E-Government Act uit 2002 als de Federal Information Security Management Act, evenals de administratieve beleidsrichtlijnen die zijn uitgebracht ter bevordering van de uitvoering van deze weten, ontwikkelt en biedt cursussen op het gebied van privacy binnen het ministerie, ondersteunt de CPLCO bij de ontwikkeling van het privacybeleid van het ministerie, stelt verslagen in verband met de privacy op voor de president en het Congres, en beoordeelt de praktijken van het ministerie met betrekking tot behandeling van informatie om te verzekeren dat dergelijke praktijken stroken met de bescherming van privacy en burgerlijke vrijheden. Het OPCL verstrekt informatie over zijn verantwoordelijkheden aan het publiek op: http://www.justice.gov/opcl.

iv) Op grond van 42 U.S.C. § 2000ee e.v. voert de Raad voor toezicht op privacy en burgerlijke vrijheden voortdurend een beoordeling uit van i) het beleid en de procedures, alsook de uitvoering daarvan, van de ministeries, instanties en onderdelen van de uitvoerende macht met betrekking tot de inspanningen om het land te beschermen tegen terrorisme, zodat de privacy en burgerlijke vrijheden worden beschermd, en ii) andere acties van de uitvoerende macht in verband met dergelijke inspanningen, om vast te stellen of dergelijke acties op passende wijze de privacy en burgerlijke vrijheden beschermen en consistent zijn met de vigerende wetgeving, regelingen en beleidsmaatregelen op het gebied van privacy en burgerlijke vrijheden. De Raad ontvangt en beoordeelt verslagen en andere informatie van de functionarissen voor privacy en burgerlijke vrijheden en geeft deze functionarissen, in voorkomend geval, aanbevelingen met betrekking tot hun activiteiten. In sectie 803 van de uitvoeringsaanbevelingen van de 9/11 Commission Act van 2007, gecodificeerd onder 42 U.S.C.§ 2000ee-1, worden de functionarissen voor privacy en burgerlijke vrijheden van acht federale instanties (waaronder de minister van Defensie, de minister van Binnenlandse Veiligheid, de directeur van de nationale inlichtingendienst en de directeur van het Central Intelligence Agency) en eventuele andere door de Raad aangewezen instanties gelast om periodiek verslagen in te dienen bij de PCLOB, onder andere over het aantal, de aard en de afhandeling van klachten over vermeende schending die door de

desbetreffende instantie zijn ontvangen. In de oprichtingsstatuten van de PCLOB wordt de Raad de opdracht gegeven deze verslagen in ontvangst te nemen en, in voorkomend geval, aanbevelingen te doen aan de functionarissen voor privacy en burgerlijke vrijheden met betrekking tot hun activiteiten.

BIJLAGE IV

Brief van de voorzitter van de Federal Trade Commission Edith Remirez

7 juli 2016

Via e-mail

Věra Jourová
Commissaris voor Justitie, Consumentenrechten en Gendergelijkheid
Europese Commissie
Wetstraat 200
1049 Brussel
BELGIË

Geachte commissaris Jourová:

De Federal Trade Commission („FTC") van de Verenigde Staten is blij met de kans om haar handhaving van het kader voor het nieuwe EU-VS-privacyschild (het „privacyschildkader" of „kader") te beschrijven. Wij zijn van mening dat het kader een cruciale rol zal spelen bij het faciliteren van privacybeschermende commerciële transacties in een wereld waarin men steeds meer met elkaar verbonden raakt. 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. De FTC zet zich reeds lange tijd in voor de grensoverschrijdende bescherming van privacy en zal aan de handhaving van het nieuwe kader een hoge prioriteit geven. Hieronder zullen we de geschiedenis van de strikte privacyhandhaving door de FTC in het algemeen beschrijven, waaronder onze wijze van handhaving van het oorspronkelijke Veiligehavenprogramma, evenals de aanpak van de FTC ten aanzien van de handhaving van het nieuwe kader.

De FTC deed haar eerste publieke toezegging het Veiligehavenprogramma te handhaven in 2000. Toen stuurde de toenmalige voorzitter van de FTC, Robert Pitofsky, de Europese Commissie een brief met de toezegging van de FTC om de privacybeginselen in het kader van het Veiligehavenprogramma krachtig te handhaven. De FTC heeft zich aan deze toezegging gehouden tijdens bijna veertig handhavingsacties, talrijke aanvullende onderzoeken en samenwerking met afzonderlijke Europese gegevensbeschermingsautoriteiten over zaken van wederzijds belang.

Nadat de Europese Commissie in november 2013 haar zorgen uitte over het beheer en de handhaving van het Veiligehavenprogramma, werden door het ministerie van Handel van de VS en de FTC besprekingen begonnen met ambtenaren van de Europese Commissie over de wijze waarop het programma zou kunnen worden versterkt. Terwijl deze besprekingen plaatsvonden, wees het Hof van Justitie van de Europese Unie op 6 oktober 2015 een arrest in de zaak *Schrems* waarin, onder andere, de beschikking van de Europese Commissie over de gepastheid van het Veiligehavenprogramma ongeldig werd verklaard. Na deze uitspraak bleven we nauw samenwerken met het ministerie van Handel en de Europese Commissie om de privacybescherming voor particulieren in de EU te verbeteren. Het privacyschildkader is een resultaat van deze voortdurende besprekingen. Net als bij het Veiligehavenprogramma verplicht de FTC zich nu ertoe dit nieuwe kader krachtdadig te handhaven. Deze toezegging wordt in deze brief nog eens herhaald.

We bevestigen onze toezegging in het bijzonder op vier hoofdgebieden: 1) het geven van prioriteit aan verwijzingen en onderzoeken; 2) de aanpak van valse of misleidende verklaringen over de aansluiting bij het privacyschild; 3) voortdurend toezicht op uitvoering van beslissingen, en 4) verbeterde contacten en handhavingssamenwerking met de gegevensbeschermingsautoriteiten in de EU. Hieronder verstrekken we gedetailleerde informatie over elk van deze toezeggingen en relevante achtergrondinformatie over de rol van de FTC bij het beschermen van de privacy van consumenten en de handhaving van de veilige haven, alsook over het bredere privacylandschap in de Verenigde Staten ([1]).

I. ACHTERGROND

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

([1]) Aanvullende informatie over federale en deelstaatwetgeving op het gebied van privacy is beschikbaar in bijlage A en een overzicht van onze recente handhavingsmaatregelen op het gebied van privacy en veiligheid is beschikbaar op de website van de FTC: https://www.ftc.gov/reports/privacy-data-security-update-2015

gegevensbescherming handhaaft de FTC een breed scala aan wetten ter bescherming van de privacy en beveiliging van consumentengegevens. De primaire wet die door de FTC wordt gehandhaafd, de FTC Act, verbiedt „oneerlijke" en „misleidende" handelingen of praktijken in het kader van of betrekking hebbend op handel ([1]). Een weergave, omissie of praktijk is misleidend als deze materieel is en consumenten die gezien de omstandigheden redelijk handelen waarschijnlijk zal misleiden ([2]). Een praktijk is 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 ([3]). Ook handhaaft de FTC specifieke wetten die informatie over gezondheid, krediet en andere financiële aangelegenheden, alsook online-gegevens van kinderen beschermen, en heeft zij regelgeving uitgevaardigd ter uitvoering van deze wetten.

De rechtsbevoegdheid van de FTC op grond van de FTC Act is van toepassing op aangelegenheden „in het kader van of betrekking hebbend op handel". De FTC heeft geen rechtsbevoegdheid op het gebied van strafrechtelijke handhaving of zaken van 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 werkelijkheid 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 ([4]). 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.

Handhaving is de spil van de benadering van de FTC in het kader van privacybescherming. De FTC heeft tot op heden meer dan 500 zaken behandeld inzake de bescherming van privacy en de beveiliging van consumentengegevens. Deze zaken hebben betrekking op zowel online- als offline-informatie en omvatten handhavingsmaatregelen tegen zowel grote als kleine bedrijven die werd verweten dat zij niet naar behoren met gevoelige consumentengegevens zijn omgegaan, de persoonsgegevens van consumenten niet hebben beveiligd, op misleidende wijze consumenten online hebben gevolgd, consumenten spam hebben verzonden, spyware of andere kwaadaardige software hebben geïnstalleerd op de computers van consumenten, het bel-me-niet register en andere telemarketingregels niet in acht hebben genomen, of onrechtmatig consumenteninformatie op mobiele apparaten hebben verzameld en gedeeld. De handhavingsacties van de FTC — in zowel de fysieke als de digitale wereld — wijzen bedrijven met kracht op de noodzaak de privacy van consumenten te beschermen.

De FTC heeft ook meerdere beleidsinitiatieven genomen die gericht waren op het verbeteren van de privacy van consumenten en die bijdragen tot haar handhavingswerkzaamheden. De FTC heeft workshops georganiseerd en rapporten uitgebracht waarin beste praktijken werden aanbevolen die onder meer gericht waren op het verbeteren van de privacy in de mobiele omgeving, het verhogen van de transparantie van de handel in gegevens door gegevensmakelaars, het maximaliseren van de voordelen van „big data" onder gelijktijdige beperking van de risico's daarvan, met name voor consumenten met een laag inkomen of die onvoldoende voorzieningen genieten, en het benadrukken van de gevolgen op het gebied van privacy en veiligheid van gezichtsherkenning en het internet der dingen.

De FTC voert ook opleidingsactiviteiten uit voor consumenten en bedrijven om de impact van haar initiatieven op het gebied van handhaving en beleidsontwikkeling te verbeteren. De FTC heeft met een reeks van instrumenten — publicaties, onlinebronnen, workshops en sociale media — voorlichtingsmateriaal verstrekt over een breed scala aan onderwerpen, waaronder mobiele apps, de privacy van kinderen en gegevensbeveiliging. De FTC is recentelijk gestart met het initiatief „Start With Security", dat nieuwe richtsnoeren voor bedrijven omvat, die zijn gebaseerd op de ervaring die de instantie heeft opgedaan met zaken over gegevensbeveiliging, alsook een reeks workshops in het hele land. Bovendien loopt de FTC al lange tijd voorop op het gebied van de voorlichting aan consumenten over elementaire computerbeveiliging. Vorig jaar werden onze website OnGuard Online en de Spaanstalige versie daarvan, Alerta en Linea, meer dan vijf miljoen keer bekeken.

B. **Juridische bescherming in de VS die ten goede komt aan EU-burgers**

Het kader zal worden uitgevoerd in de context van het bredere privacylandschap van de VS, waarin EU-consumenten op een aantal manieren worden beschermd.

([1]) 15 U.S.C. § 45(a).

([2]) Zie FTC Policy Statement on Deception, bijlage bij Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), beschikbaar op: https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception

([3]) Zie 15 U.S.C § 45(n); FTC Policy Statement on Unfairness, bijlage bij Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), beschikbaar op: https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness

([4]) Zie California Dental Ass'n v. FTC, 526 U.S. 756 (1999).

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, waaronder restitutie, die voor de bescherming van binnenlandse consumenten beschikbaar zijn, ook aanwenden ten behoeve van de bescherming van buitenlandse consumenten.

De handhavingsactiviteiten van de FTC hebben dus aanzienlijke voordelen voor zowel Amerikaanse als buitenlandse consumenten. Onze zaken ter handhaving van sectie 5 van de FTC Act hebben bijvoorbeeld de privacy van zowel Amerikaanse als buitenlandse consumenten beschermd. In een zaak tegen een informatiemakelaar, Accusearch, stelde de FTC dat de verkoop van vertrouwelijke telefoongegevens door het bedrijf aan derden zonder medeweten of toestemming van de consument een oneerlijke, met sectie 5 van de FTC Act strijdige praktijk was. Accusearch verkocht informatie over zowel Amerikaanse als buitenlandse consumenten ([1]). De rechtbank legde Accusearch een dwangmaatregel tot rechtsherstel op waarbij, onder andere, de marketing of verkoop van persoonsgegevens van consumenten zonder schriftelijke toestemming werd verboden, tenzij deze gegevens rechtmatig werden verkregen uit openbaar beschikbare informatie en gelastte de terugbetaling van bijna 200 000 USD ([2]).

De schikking van de FTC met TRUSTe is een ander voorbeeld. Deze verzekert dat consumenten, waaronder die in de Europese Unie, kunnen vertrouwen op verklaringen van een wereldwijd opererende zelfregulerende organisatie over haar beoordeling en certificering van binnenlandse en buitenlandse onlinediensten ([3]). Het is van belang dat ons optreden jegens TRUSTe ook in ruimere zin het zelfreguleringssysteem op het gebied van privacy versterkt door ervoor te zorgen dat entiteiten die een belangrijke rol spelen in zelfreguleringsstelsels, waaronder grensoverschrijdende privacykaders, verantwoording af moeten leggen.

De FTC handhaaft ook 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 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 bepaalde andere federale en deelstaatswetgeving inzake consumentenbescherming en privacy EU-consumenten nog meer voordelen bieden.

C. **Handhaving in het kader van de veilige haven**

Als onderdeel van haar handhavingsprogramma inzake privacy en beveiliging heeft de FTC er ook naar gestreefd EU-consumenten te beschermen door handhavingsmaatregelen te nemen met betrekking tot schendingen van de veilige haven. De FTC heeft in het kader van de veilige haven 39 handhavingsactiviteiten uitgevoerd: in 36 zaken was er sprake van vermeend valse certificeringsverklaringen en in drie gevallen — tegen Google, Facebook en Myspace — ging het om vermeende schendingen van de Veiligehavenbeginselen ([4]). Deze zaken laten zien dat ten aanzien van certificering handhavend kan worden opgetreden en wat de gevolgen van niet-naleving zijn. Bij beschikking vastgestelde compromissen („consent orders") met een geldigheidsduur van twintig jaar verplichten Google, Facebook en Myspace ertoe om uitgebreide privacyprogramma's uit te voeren die redelijkerwijs zo moeten zijn ontworpen dat zij de privacyrisico's in verband met de ontwikkeling en het beheer van nieuwe en bestaande producten en diensten aanpakken en de privacy en vertrouwelijkheid van persoonsgegevens beschermen. De uitgebreide privacyprogramma's waartoe op grond van deze beschikkingen opdracht is gegeven, moeten voorzienbare materiële risico's vaststellen en in controles voorzien om deze risico's aan te pakken. Ook moeten de bedrijven zich onderwerpen aan voortdurende, onafhankelijke beoordelingen van hun privacyprogramma's, die bij de FTC moeten worden ingediend. Voorts is het bedrijven op grond van deze beschikkingen verboden een verkeerde voorstelling te geven van hun privacypraktijken en hun deelname aan privacy- of beveiligingsprogramma's. Dit verbod zou op de handelingen en praktijken van bedrijven op grond van het nieuwe privacyschildkader ook van toepassing zijn. De FTC kan deze beschikkingen handhaven door middel van civiele sancties. Google betaalde in 2012 zelfs een civielrechtelijke recordboete van 22,5 miljoen USD naar aanleiding van beschuldigingen dat het bedrijf het haar betreffende besluit had geschonden. Deze FTC-beschikkingen dragen dus bij tot de bescherming van meer dan een miljard consumenten wereldwijd, waarvan er honderden miljoenen in Europa wonen.

([1]) Zie Office of the Privacy Commissioner of Canada, Complaint under PIPEDA against Accusearch, Inc., doing business as Abika.com, https://www.priv.gc.ca/cf-dc/2009/20090090731_e.asp. Het bureau van de Privacy Commissioner van Canada diende een memorie in als amicus curiae in de beroepszaak tegen de FTC-maatregel en voerde een eigen onderzoek uit, naar aanleiding waarvan werd geconcludeerd dat de praktijken van Accusearch ook de Canadese wetgeving schonden.

([2]) Zie *FTC v. Accusearch, Inc.*, No. 06CV015D (D. Wyo. Dec. 20, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

([3]) Zie *In the Matter of True Ultimate Standards Everywhere, Inc.*, No. C-4512 (F.T.C. 12 maart 2015) (decision and order), beschikbaar op: https://www.ftc.gov/system/files/documents/cases/150318trust-edo.pdf

([4]) Zie *In the Matter of Google, Inc.*, No. C-4336 (F.T.C. Oct. 13 2011) (decision and order), beschikbaar op: https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *In the Matter of Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012) (decision and order), beschikbaar op: https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; *In the Matter of Myspace LLC*, No. C-4369 (F.T.C. Aug. 30, 2012) (decision and order), beschikbaar op: https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace

Een ander aandachtspunt van FTC vormden valse of misleidende verklaringen over deelname aan het Veiligehavenprogramma. De FTC neemt deze beweringen zeer serieus. In 2011 bijvoorbeeld maakte de FTC in *FTC v. Karnani* een zaak aanhangig tegen een internetmarketeer in de Verenigde Staten en stelde dat hij en zijn bedrijf Britse consumenten op bedrieglijke wijze lieten geloven dat het bedrijf gevestigd was in het Verenigd Koninkrijk, onder meer door gebruik te maken van de internetextensie.uk en te verwijzen naar de Britse valuta en de Britse posterijen ([1]). Bij de ontvangst van de producten werden de consumenten echter geconfronteerd met onverwachte invoerheffingen, garanties die niet geldig waren in het Verenigd Koninkrijk en kosten in verband met het verkrijgen van terugbetaling. De FTC stelde tevens dat de gedaagden consumenten misleidden ten aanzien van hun deelname aan het Veiligehavenprogramma. Alle consumenten die het slachtoffer werden van deze praktijken woonden in het Verenigd Koninkrijk.

Veel van onze andere handhavingszaken in het kader van de veilige haven hadden betrekking op organisaties die zich aansloten bij het Veiligehavenprogramma, maar die nalieten hun jaarlijkse certificering te vernieuwen terwijl ze zich toch bleven voordoen als lid. Zoals hierna verder zal worden besproken, verplicht de FTC zich er ook toe om valse beweringen van deelname aan het privacyschildkader aan te pakken. Deze strategische handhavingsactiviteiten vormen een aanvulling op de toegenomen werkzaamheden van het ministerie van Handel om de naleving van de programmavereisten voor certificering en hercertificering te controleren, het toezicht door het ministerie op de daadwerkelijke naleving, onder meer door deelnemers aan het kader vragenlijsten voor te leggen, en de toegenomen inspanningen van het ministerie om de valsheid van beweringen over deelname aan het kader en misbruik van het keurmerk van het kader vast te stellen ([2]).

II. HET VERLENEN VAN PRIORITEIT AAN VERWIJZINGEN EN ONDERZOEKEN

Net zoals bij het Veiligehavenprogramma zegt de FTC ook toe prioriteit te geven aan zaken die door de EU-lidstaten op grond van het privacyschild worden voorgelegd. Ook geven wij prioriteit aan kwesties in verband met de niet-naleving van zelfreguleringsrichtsnoeren in verband met het privacyschildkader die worden voorgelegd door op het gebied van privacy zelfregulerende organisaties en andere onafhankelijke instanties voor geschillenbeslechting.

Om verwijzingen van EU-lidstaten op grond van het kader te vereenvoudigen, werkt de FTC aan een gestandaardiseerd verwijzingsproces en het opstellen van richtsnoeren voor EU-lidstaten 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 zal instellen 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 verwijzing uit een EU-lidstaat of van een zelfregulerende organisatie kan de FTC een aantal acties ondernemen om de aangekaarte problemen aan te pakken. We kunnen bijvoorbeeld het privacybeleid van het bedrijf onderzoeken, rechtstreeks bij het bedrijf 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 voorlichting van consumenten en bedrijven nuttig kan zijn en, in voorkomend geval, een handhavingsprocedure starten.

De FTC zegt tevens toe informatie uit te wisselen over verwijzingen 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,

([1]) Zie *FTC v. Karnani*, No. 2:09-cv-05276 (C.D. Cal. May 20, 2011) (stipulated final order), beschikbaar op: https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; zie ook Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, http://www.business.ftc.gov/blog/2011/06/around-world-shady-ways (June 9, 2011).

([2]) Brief van Ken Hyatt, waarnemend onderminister van Handel voor Internationale Handel, International Trade Administration, aan Věra Jourová, Commissaris voor Justitie, Consumentenrechten en Gendergelijkheid.

te verhogen. Wanneer een verwijzende handhavingsinstantie met het oog op het instellen van zijn 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 ([1]). 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 ([2]).

De FTC geeft niet alleen voorrang aan verwijzingen in het kader van het privacyschild van EU-lidstaten en op het gebied van privacy zelfregulerende organisaties ([3]), maar verplicht zich ook ertoe om mogelijke schendingen van het kader in voorkomend geval op eigen initiatief te onderzoeken met behulp van een reeks hulpmiddelen.

Gedurende meer dan tien jaar heeft de FTC een solide programma uitgevoerd inzake onderzoeken naar privacy- en beveiligingskwesties waarbij commerciële organisaties betrokken zijn. Als onderdeel van deze onderzoeken heeft de FTC stelselmatig onderzocht of de desbetreffende entiteit beweringen deed met betrekking tot het Veiligehaveprogramma. Als de entiteit dergelijke beweringen deed en uit het onderzoek bleek dat de Veiligehavenbeginselen inzake de privacy kennelijk waren geschonden, dan nam de FTC de beschuldigingen van schending van de Veiligehavenbeginselen in aanmerking bij haar handhavingsmaatregelen. We zullen deze proactieve aanpak binnen het nieuwe kader voortzetten. Het moet worden benadrukt dat de onderzoeken die uiteindelijk tot publieke handhavingsacties leiden maar een klein deel zijn van het totale aantal onderzoeken dat door de FTC wordt uitgevoerd. Veel FTC-onderzoeken worden gesloten omdat er geen duidelijke schending van de wet kan worden geconstateerd. Aangezien FTC-onderzoeken niet-openbaar en vertrouwelijk zijn, wordt het sluiten van een onderzoek vaak niet openbaar gemaakt.

De bijna veertig handhavingsacties die door de FTC zijn uitgevoerd met betrekking tot het Veiligehavenprogramma vormen het bewijs dat deze instantie zich inzet om grensoverschrijdende privacyprogramma's proactief te handhaven. De FTC doet onderzoek naar mogelijke schendingen van het kader als onderdeel van de privacy- en veiligheidsonderzoeken die we regelmatig uitvoeren.

III. AANPAK VAN VALSE OF MISLEIDENDE VERKLARINGEN OVER HET LIDMAATSCHAP VAN HET PRIVACYSCHILD

Zoals hiervoor al is opgemerkt, onderneemt de FTC actie tegen entiteiten die onjuiste verklaringen afleggen over hun deelname aan het kader. De FTC geeft prioriteit aan verwijzingen van het ministerie van Handel over organisaties waarvan het ministerie vaststelt dat zij ten onrechte voorgeven aan het kader deel te nemen of die het keurmerk van het kader zonder toestemming gebruiken.

Daarnaast merken we op dat indien in het kader van het privacybeleid van een organisatie wordt beloofd dat zij voldoet aan de privacyschildbeginselen, het feit dat de organisatie zich niet bij het ministerie van Handel registreert of haar registratie daar niet verlengt, op zichzelf waarschijnlijk geen reden vormt om de organisatie te vrijwaren van de handhaving door de FTC van deze toezegging.

([1]) 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.

([2]) In de boekjaren 2012-2015 maakte de FTC bijvoorbeeld gebruik van haar bevoegdheid op grond van de U.S Safe WEB Act om informatie te delen in reactie op bijna zestig verzoeken van buitenlandse instanties en deed zij bijna zestig civielrechtelijke onderzoeksverzoeken (vergelijkbaar met administratieve dagvaardingen) om te helpen bij 25 buitenlandse onderzoeken.

([3]) 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 het privacyschild 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. Particulieren in de EU kunnen gebruikmaken van hetzelfde klachtensysteem dat beschikbaar is voor Amerikaanse burgers om een klacht in te dienen bij de FTC op: www.ftc.gov/complaint. Voor individuele klachten in het kader van het privacyschild kan het voor particulieren in de EU echter zeer nuttig zijn om klachten in te dienen bij de gegevensbeschermingsinstantie in hun lidstaat of bij een alternatieve geschillenbeslechtingsinstantie.

IV. TOEZICHT OP DE UITVOERING VAN BESLUITEN

De FTC bevestigt tevens haar toezeggingen om toezicht te houden op de uitvoering van handhavingsbesluiten teneinde de naleving van het privacyschildkader te verzekeren.

We zullen tot naleving van het kader verplichten door in de toekomst in besluiten van de FTC in de context van het privacyschild een verscheidenheid aan dwingende bepalingen op te nemen. Daarbij gaat het onder meer om het verbod van onjuiste verklaringen met betrekking tot het kader en andere privacyprogramma's wanneer deze de basis vormen voor de onderliggende FTC-maatregelen.

De zaken van de FTC waarin het oorspronkelijke Veiligehavenprogramma werd gehandhaafd, zijn in dit opzicht leerzaam. In de 36 gevallen waarin sprake was van valse of misleidende beweringen over de certificering in het kader van de Veilige Haven werd de gedaagde telkens verboden om misleidende verklaringen af te leggen over zijn deelname aan het Veiligehavenprogramma of een ander privacy- of beveiligingsprogramma en werd het bedrijf ertoe verplicht de FTC nalevingsverslagen te overleggen. In gevallen waarin sprake was van schending van de Veiligehavenbeginselen inzake de privacybescherming zijn bedrijven ertoe verplicht uitgebreide privacyprogramma's uit te voeren en gedurende twintig jaar deze programma's jaarlijks door onafhankelijke derden te laten beoordelen en de FTC van deze beoordeling in kennis te stellen.

Schendingen van de administratieve bevelen van de FTC kunnen leiden tot civiele boeten tot maximaal 16 000 USD per schending of 16 000 USD per dag in geval van voortgaande schending ([1]), 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 stelselmatig toezicht op de naleving van veiligehavenbesluiten, net zoals bij al haar besluiten het geval is. De FTC neemt de handhaving van haar besluiten in het kader van privacy en gegevensbeveiliging serieus en neemt indien nodig handhavingsmaatregelen. Zo betaalde Google, zoals hierboven opgemerkt, een civielrechtelijke boete van 22,5 miljoen USD in het kader van een schikking, na beschuldigingen dat de onderneming het jegens haar genomen FTC-besluit had geschonden. 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.

Tot slot zal de FTC een onlinelijst blijven bijhouden van bedrijven waarop bevelen van toepassing zijn die zijn uitgevaardigd in verband met de handhaving van zowel het veiligehavenprogramma als het nieuwe privacyschildkader ([2]). Daarnaast verplichten de privacyschildbeginselen bedrijven waarop een FTC- of gerechtelijk bevel op grond van niet-naleving van de beginselen van toepassing is, er thans toe om eventuele in verband met het kader relevante passages in een bij de FTC ingediend nalevings- of beoordelingsverslag openbaar te maken, voor zover dat strookt met de wet- en regelgeving op het gebied van vertrouwelijkheid.

V. INTERACTIE MET EUROPESE GEGEVENSBESCHERMINGSAUTORITEITEN EN SAMENWERKING OP HET GEBIED VAN HANDHAVING

De FTC erkent de belangrijke rol die Europese gegevensbeschermingsautoriteiten spelen met betrekking tot de naleving van het kader en moedigt meer raadpleging en samenwerking op het gebied van handhaving aan. De FTC zegt niet alleen toe om met de verwijzende gegevensbeschermingsautoriteiten te overleggen over op een specifieke zaak betrekking hebbende aangelegenheden, maar verplicht zich er ook toe om deel te nemen aan periodieke bijeenkomsten met daartoe aangewezen vertegenwoordigers van de Groep artikel 29 teneinde in het algemeen te bespreken hoe de samenwerking op het gebied van handhaving met betrekking tot het kader kan worden verbeterd. De FTC zal, samen met het ministerie van Handel, de Europese Commissie en vertegenwoordigers van de Groep artikel 29, ook deelnemen aan de jaarlijkse beoordeling van het kader, 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. Met name heeft de FTC, samen met handhavingspartners in de Europese Unie en wereldwijd, vorig jaar een waarschuwingssysteem gelanceerd binnen het Global Privacy Enforcement Network („GPEN") om informatie te delen over onderzoeken en coördinatie op het gebied van handhaving te bevorderen. Dit waarschuwingsinstrument van het GPEN kan bijzonder nuttig zijn in de context van het privacyschildkader. De FTC en Europese gegevensbeschermingsautoriteiten kunnen het gebruiken voor coördinatie in verband met het kader en andere privacyonderzoeken,

([1]) 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.

([2]) Zie FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=251

onder meer als startpunt voor het delen van informatie, om zo burgers een gecoördineerde en doeltreffender privacybescherming te bieden. We kijken uit naar de voortzetting van de samenwerking met de deelnemende EU-instanties om het GPEN-waarschuwingssysteem breder in te zetten en andere instrumenten te ontwikkelen om de samenwerking te bevorderen op het gebied van handhaving in privacykwesties, waaronder die welke betrekking hebben op het kader.

De FTC is verheugd haar toezegging het privacyschildkader te zullen handhaven, te bevestigen. Ook kijken wij uit naar het voortzetten van de samenwerking met onze collega's uit de EU om de privacy van consumenten aan weerszijden van de Atlantische Oceaan te beschermen.

Met vriendelijke groet,

Edith Ramirez

Voorzitter

Aanhangsel A

Het EU-VS-privacyschildkader in zijn context: een overzicht van de situatie op het gebied van privacy en veiligheid in de VS

De bescherming die het EU-VS-privacyschildkader biedt („het kader"), moet worden gezien in de context van de ruimere privacybescherming op grond van het Amerikaanse rechtssysteem in zijn geheel. Allereerst beschikt de Amerikaanse Federal Trade Commission („FCT") over een degelijk programma inzake privacy en beveiliging van persoonsgegevens op het gebied van handelspraktijken, dat consumenten wereldwijd beschermt. In de tweede plaats is de situatie op het gebied van de bescherming van de privacy en de veiligheid van consumenten in de Verenigde Staten sinds 2000, toen het oorspronkelijke VS-EU-veiligehavenprogramma werd vastgesteld, aanzienlijk geëvolueerd. Sindsdien zijn er op federaal en deelstaatniveau veel veiligheidswetten vastgesteld en is de publieke en particuliere geschillenbeslechting ter handhaving van privacyrechten aanzienlijk toegenomen. Het brede toepassingsgebied van de wettelijke bescherming in de VS op het gebied van de privacy en veiligheid van consumenten in het kader van praktijken inzake commerciële gegevens vult de bescherming aan die het nieuwe kader particulieren in de EU biedt.

I. HET ALGEMENE PROGRAMMA VAN DE FTC VOOR DE HANDHAVING VAN PRIVACY EN VEILIGHEID

De FTC is de voornaamste Amerikaanse instantie op het gebied van consumentenbescherming die zich bezighoudt met privacy in de commerciële sector. De FTC is bevoegd om vervolging in stellen naar aanleiding van oneerlijk of misleidende handelingen of praktijken die de privacy van consumenten schenden, alsook om meer specifieke privacywetten te handhaven op het gebied van de bescherming van bepaalde financiële informatie en informatie inzake gezondheid, informatie over kinderen en informatie die wordt gebruikt om bepaalde subsidiabiliteitsbesluiten inzake consumenten te nemen.

De FTC heeft een ongeëvenaarde ervaring met de bescherming van de privacy van consumenten. Met handhavingsmaatregelen van de FTC zijn onrechtmatige praktijken in zowel de offline- als de onlineomgeving aangepakt. Zo heeft de FTC handhavingsmaatregelen genomen ten aanzien van zeer bekende bedrijven als Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC, en Snapchat, maar ook ten aanzien van minder bekende bedrijven. De FTC heeft bedrijven vervolgd die werden beschuldigd van het sturen van spam naar consumenten, het installeren van spyware op computers, het nalaten de persoonsgegevens van consumenten te beveiligen, het misleidend online volgen van consumenten, het schenden van de privacy van kinderen, het onrechtmatig verzamelen van informatie op de mobiele apparatuur van consumenten, en het niet-beveiligen van met het internet verbonden apparatuur voor het opslaan van persoonsgegevens. De meeste uitspraken naar aanleiding van die procedures hielden een permanent toezicht door de FTC gedurende een periode van twintig jaar, een verbod tot verdere schendingen van het recht en een aanzienlijke voorwaardelijk geldboete voor het geval de uitspraak niet zou worden nageleefd, in. ([1]) Het is een belangrijk gegeven dat uitspraken van de FTC niet alleen de individuen beschermen die over een probleem hebben geklaagd: zij bieden juist alle consumenten bescherming die in de toekomst met de betreffende aangelegenheid te maken hebben. In een grensoverschrijdend kader is de FTC bevoegd om consumenten wereldwijd te beschermen tegen praktijken die in de Verenigde Staten plaatsvinden ([2]).

Tot op heden heeft de FTC meer dan 130 zaken aangespannen op het gebied van spam en spyware, meer dan 120 „Belme niet"-zaken aangespannen op het gebied van telemarketing, meer dan 100 acties ondernomen op grond van de Fair Credit Reporting Act, bijna 60 zaken aangespannen op het gebied van gegevensbeveiliging, meer dan 50 algemen acties ondernomen op het gebied van privacy, bijna 30 zaken aangespannen wegens schendingen van de Gramm-Leach-Bliley Act en meer dan 20 acties ondernomen ter handhaving van de Children's Online Privacy Protection Act („COPPA") ([3]). Daarnaast heeft de FTC ook waarschuwingsbrieven verstuurd en gepubliceerd ([4]).

([1]) Iedere entiteit die geen gevolg geeft aan een uitspraak van de FTC kan een civielrechtelijke sanctie worden opgelegd ten belope van maximaal 16 000 USD per schending, of 16 000 USD per dag in geval van voortgaande schending. Zie 15 U.S.C. § 45(l); 16 C.F.R. § 1.98(c).

([2]) Het Congres heeft uitdrukkelijk bevestigd dat de FTC bevoegd is om rechtsmiddelen aan te wenden, met inbegrip van restitutie, ten aanzien van alle handelingen of praktijken in het kader van buitenlandse handel die 1) in de Verenigde Staten redelijk voorzienbare schade veroorzaken of waarschijnlijk zullen veroorzaken of 2) gepaard gaan met materiële gedragingen in de Verenigde Staten. Zie 15 U. S.C. § 45(a)(4).

([3]) In een aantal van de procedures die de FTC voerde op het gebied van privacy en gegevensbescherming werden bedrijven ervan beschuldigd zich aan zowel misleidende als oneerlijke praktijken schuldig te hebben gemaakt; deze gevallen betreffen soms ook vermeende schendingen van meervoudige wetgeving, zoals de Fair Credit Reporting Act, de Gramm-Leach-Bliley Act, en COPPA.

([4]) Zie, bijvoorbeeld, Persbericht, Federal Trade Commissie, FTC Warns Children's App Maker BabyBus About Potential COPPA Violations (Dec. 22, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; Persbericht, Federal Trade Commission, FTC Warns Data Broker Operations of Possible Privacy Violations (May 7, 2013), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations; Persbericht, Federal Trade Commission, FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act (Apr. 3, 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may

Als onderdeel van haar traditie van krachtige privacyhandhaving heeft de FTC ook met regelmaat in de gaten gehouden of het Veiligehavenprogramma niet wordt geschonden. Sinds het Veiligehavenprogramma werd vastgesteld, heeft de FTC uit eigen beweging diverse onderzoeken ingesteld naar de naleving van de Veiligehavenbeginselen en 39 zaken ingeleid tegen VS-ondernemingen die de Veiligehavenbeginselen hadden geschonden. De FTC zal deze proactieve benadering voortzetten door van de handhaving van het nieuwe kader een prioriteit te maken.

II. BESCHERMING VAN DE PRIVACY VAN CONSUMENTEN OP FEDERAAL EN DEELSTAATNIVEAU

Het overzicht van de handhaving van de Veiligehavenregeling, dat als een bijlage bij het adequaatheidsbesluit inzake de Veilige Haven van de Commissie verschijnt, biedt een samenvatting van een groot aantal van de privacywetten op federaal of deelstaatniveau die in 2000, toen het Veilighavenprogramma werd vastgesteld, van kracht waren ([1]). Toendertijd werd het commercieel verzamelen en gebruiken van persoonlijke informatie niet alleen door sectie 5 van de FTC Act, maar ook door veel andere federale wetten geregeld, waaronder: de Cable Communications Policy Act, de Driver's Privacy Protection Act, de Electronic Communications Privacy Act, de Electronic Funds Transfer Act, de Fair Credit Reporting Act, de Gramm-Leach-Bliley Act, de Right to Financial Privacy Act, de Telephone Consumer Protection Act, en de Video Privacy Protection Act. Veel deelstaten hadden op deze gebieden ook nog analoge wetgeving.

Sinds 2000 hebben er op federaal en deelstaatniveau talrijke ontwikkelingen plaatsgevonden die consumenten extra privacybescherming bieden ([2]). Op federaal niveau heeft de FTC bijvoorbeeld in 2013 de COPPA-regeling gewijzigd zodat de persoonlijke informatie van kinderen op een aantal punten extra wordt beschermd. De FTC heeft ook twee regelingen opgesteld die uitvoering geven aan de Gramm-Leach-Bliley Act — the Privacy Rule en de Safeguards Rule — die financiële instellingen ([3]) ertoe verplichten inzage te verschaffen in hun praktijken op het gebied van het delen van informatie en om een uitgebreid programma inzake informatiebeveiliging uit te voeren ter bescherming van consumenteninformatie ([4]). Zo ook vult de Fair and Accurate Credit Transactions Act („FACTA"), die in 2003 van kracht werd, reeds lang bestaande Amerikaanse wetgeving op het gebied van krediet aan door vereisten vast te stellen voor het verbergen, delen en wissen van bepaalde gevoelige financiële gegevens De FTC heeft in het kader van de FACTA een aantal regels uitgevaardigd over, onder meer, het recht van consumenten op een gratis jaarlijks kredietrapport, vereisten inzake het veilig wissen van informatie inzake consumentenrapporten, het recht van consumenten om zich te verzetten tegen de ontvangst van bepaalde aanbiedingen op het gebied van krediet en verzekeringen, het recht van consumenten om zich te verzetten tegen het gebruik van informatie die door een gelieerde onderneming wordt verstrekt voor het op de markt brengen van haar producten en diensten, en het vereiste voor financiële instellingen en crediteurs om programma's op het gebied van de opsporing en preventie van identiteitsdiefstal uit te voeren ([5]). Daarnaast zijn de op grond van de Health Insurance Portability and Accountability Act uitgevaardigde regels in 2013 herzien door aanvullende waarborgen toe te voegen ter bescherming van de privacy en beveiliging van persoonlijke gezondheidsinformatie ([6]). Ook zijn er regels ter bescherming van consumenten tegen ongewenste telemarketing-telefoongesprekken, robocalls, en spam van kracht geworden Het Congres heeft ook wetgeving aangenomen die bepaalde ondernemingen die gezondheidsinformatie verzamelen ertoe verplicht consumenten in geval van een inbreuk dienaangaande een kennisgeving te doen toekomen ([7]).

Ook staten zijn zeer actief geweest met het aannemen van wetgeving op het gebied van privacy en beveiliging. Sinds 2000 hebben 47 staten, het District of Columbia, Guam, Puerto Rico en de Maagdeneilanden wetten aangenomen die

([1]) Zie ministerie van handel van de VS, Safe Harbor Enforcement Overview, https://build.export.gov/main/safeharbor/eu/eg main 018481
([2]) Zie voor een meer uitgebreide samenvatting van de wettelijke bescherming in de Verenigde Staten: Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (5e druk 2015).
([3]) Financiële instellingen worden op grond van de Gramm-Leach-Bliley Act zeer ruim gedefinieerd en omvatten daar alle ondernemingen die „zeer actief zijn" („significantly engaged") op het gebied van het aanbieden van financiële producten en diensten. Daarbij gaat het bijvoorbeeld om ondernemingen die checks innen, verstrekkers van flitskredieten, niet-bancaire geldverstrekkers, hypotheekmakelaars, taxateurs van roerende of onroerend privé-goederen en belastingadviseurs.
([4]) Op grond van de Consumer Financial Protection Act van 2010 („CFPA"), Titel X van Pub. L. 111-203, 124 Stat. 1955 (21 juli 2010) (ook bekend als de Dodd-Frank Wall Street Reform and Consumer Protection Act), werd het grootste deel van de regelgevingsbevoegdheid van de FTC uit hoofde van de Gramm-Leach-Bliley Act overgedragen aan het Consumer Financial Protection Bureau („CFPB"). De FTC behoudt de handhavingsbevoegdheid uit hoofde van de Gramm-Leach-Bliley Act alsook de regelgevingsbevoegdheid in het kader van de Safeguards Rule en beperkte regelgevingsbevoegdheid uit hoofde van de Privacy Rule ten aanzien van autohandelaren.
([5]) Op grond van de CFPA deelt de FTC haar handhavingsrol in het kader van de FCRA met het CFPB, maar is de regelgevingsbevoegdheid grotendeels overgedragen aan het CFPB (met uitzondering van de Red Flags en Disposal Rules).
([6]) Zie 45 C.F.R. punten 160, 162, 164.
([7]) Zie bijvoorbeeld, American Recovery & Reinvestment Act van 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) en relevante regelingen, 45 C.F.R. §§ 164.404-164.414; 16 C.F.R. punt 318.

ondernemingen ertoe verplichten om natuurlijke personen in kennis te stellen van inbreuken op persoonlijke informatie ([1]). Ten minste 32 staten en Puerto Rico hebben wetten inzake het wissen van gegevens, waarin vereisten zijn vastgesteld met betrekking tot de vernietiging of het wissen van persoonlijke informatie ([2]). Een aantal staten heeft ook algemene wetten inzake gegevensbeveiliging ingevoerd. Daarnaast heeft Californië diverse privacywetten ingevoerd, waaronder een wet die ondernemingen verplicht een privacybeleid te voeren en hun „Do Not Track"-praktijken openbaar te maken ([3]), een „Shine the Ligt"-wet, die brokers tot meer transparantie verplicht ([4]), en een wet die een „wistoets" verplicht stelt, waarmee minderjarigen om het wissen van bepaalde informatie op sociale media kunnen verzoeken ([5]). Op grond van deze wetten hebben de federale overheid en de overheid van de deelstaten aanzienlijke boeten opgelegd aan ondernemingen die hebben nagelaten de privacy en de persoonlijke informatie van consumenten te beschermen ([6]).

Door particulieren gevoerde processen hebben ook tot gunstige uitspraken en regelingen geleid die consumenten aanvullende bescherming van privacy en beveiliging van gegevens bieden. Zo stemde Target er in 2015 mee in om 10 miljoen USD te betalen als onderdeel van een schikking met consumenten die aanvoerden dat door een wijdverspreide inbreuk op gegevens ook inbreuk op hun persoonlijke financiële informatie was gemaakt. In 2013 stemde AOL ermee in om 5 miljoen USD te betalen als onderdeel van een schikking inzake een collectieve vordering in verband met het beweerlijk onvoldoende niet-identificeerbaar maken van openbaar gemaakte zoekopdrachten van honderdduizenden AOL-leden. Daarnaast keurde een federale rechtbank de betaling van 9 miljoen USD door Netflix goed voor het in strijd met de Video Privacy Protection Act van 1988 bewaren van de registratie van de verhuur. Federale rechtbanken in Californië keurden twee afzonderlijke schikkingen met Facebook goed, een ten bedrage van 20 miljoen USD en een ten bedrage van 9,5 miljoen USD, waarbij het ging om het verzamelen, gebruiken en delen door de onderneming van de persoonlijke informatie van haar gebruikers. En in 2008 keurde een rechtbank in Californië een schikking ten bedrage van 20 miljoen USD goed met LensCrafters vanwege de onrechtmatige openbaarmaking van medische gegevens van consumenten.

Kortom, de Verenigde Staten bieden de consument, zoals dit overzicht laat zien, aanzienlijke wettelijke bescherming op het gebied van privacy en veiligheid. Het nieuwe Privacyschildkader, dat particulieren in de EU serieuze waarborgen biedt, zal functioneren tegen deze bredere achtergrond waarbij de bescherming van de privacy en veiligheid van consumenten een belangrijke prioriteit blijft.

([1]) Zie bijvoorbeeld, National Conference of State Legislatures („NCSL"), *State Security Breach Notification Laws* (Jan. 4, 2016), beschikbaar op: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

([2]) NCSL, *Data Disposal Laws* (Jan. 12, 2016), beschikbaar op: http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx

([3]) Cal. Bus. & Professional Code §§ 22575-22579.

([4]) Cal. Civ. Code §§ 1798.80-1798.84.

([5]) Cal. Bus. & Professional Code § 22580-22582.

([6]) Zie Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (Feb. 17, 2014), beschikbaar op http://www.computerworld.com/s/article/9246393/Jay_Cline_U.S._takes_the_gold_in_doling_out_privacy_fines?taxonomyId=17&pageNumber=1

BIJLAGE V

Brief van de Amerikaanse minister van Vervoer Anthony Foxx

19 februari 2016

Commissaris Vera Jourová
Europese Commissie
Wetstraat 200
1049 Brussel
BELGIË

Betreft: EU-VS-privacyschildkader

Geachte commissaris Jourová:

Het Amerikaanse ministerie van Vervoer (het „ministerie") stelt het op prijs zijn rol bij de handhaving van het EU-VS-privacyschildkader te kunnen beschrijven. Dit kader speelt een cruciale rol bij de bescherming van persoonsgegevens die bij commerciële transacties worden verstrekt in 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.

Het ministerie zegde meer dan vijftien jaar geleden in een brief aan de Europese Commissie voor het eerst in het openbaar toe te zullen meewerken aan de handhaving van het Veiligehavenkader. Het ministerie beloofde in die brief de Veiligehavenbeginselen voor de privacybescherming krachtig te zullen handhaven. Het ministerie blijft deze toezegging nakomen en in deze brief wordt zij nogmaals in herinnering gebracht.

Het ministerie hernieuwt zijn toezegging in het bijzonder op de volgende vier gebieden: 1) het verlenen van prioriteit aan het onderzoek van vermeende schendingen van het privacyschild; 2) passende handhavingsmaatregelen tegen entiteiten die valse of misleidende beweringen doen over privacyschildcertificering; en 3) het houden van toezicht op de uitvoering en de openbaarmaking van handhavingsbevelen inzake schendingen van het privacyschild. 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 het privacyschildkader.

I. 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 of een oneerlijke mededingingsmethode te gebruiken" bij de verkoop van luchtvervoer die leidt tot of kan leiden tot schade bij de consument. Sectie 41712 volgt hetzelfde patroon als sectie 5 van de Federal Trade Commission (FTC) Act (15 U.S.C. 45). Zoals wij de wet betreffende oneerlijke of misleidende praktijken uitleggen, is het een luchtvaartmaatschappij of reisbureau verboden om: 1) de voorwaarden van het eigen privacybeleid te schenden, of 2) persoonlijke informatie te verzamelen of openbaar te maken op een manier die in strijd is met openbaar beleid of goede zeden of die aanzienlijke schade veroorzaakt voor de consument, die niet wordt gecompenseerd door eventuele voordelen. Volgens onze interpretatie van sectie 41712 is het luchtvaartmaatschappijen en reisbureaus tevens verboden om: 1) een door het ministerie uitgevaardigd voorschrift te schenden waarin specifieke privacypraktijken als oneerlijk of misleidend worden aangemerkt; of 2) de Children's Online Privacy Protection Act (COPPA) of FTC-voorschriften ter de uitvoering van de COPPA te schenden. Op grond van federale wetgeving heeft het ministerie 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 privacybeginselen van het privacyschildkader, 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 privacybeginselen van het privacyschildkader en dit vervolgens niet doet, handelt deze maatschappij of dit bureau dan ook in strijd met sectie 41712.

B. **Handhavingspraktijken**

Het bureau voor handhaving en procedures betreffende de luchtvaart van het ministerie (bureau voor handhaving betreffende de luchtvaart) 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 individuele 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 258 ([1]).

Indien er in een zaak geen redelijke en passende schikking wordt bereikt, heeft het bureau voor handhaving betreffende de luchtvaart 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 27 500 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 bureau voor handhaving betreffende de luchtvaart 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 privacybeginselen van het privacyschild 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.

Het ministerie handhaaft met betrekking tot luchtvaartmaatschappijen tevens andere specifieke wetgeving waarvan de bescherming ook consumenten buiten de VS omvat, zoals de COPPA. De COPPA verplicht exploitanten van op kinderen gerichte websites en onlinediensten of websites voor het algemene publiek die doelbewust persoonlijke informatie 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 HET PRIVACYSCHILD

Als een luchtvaartmaatschappij of reisbureau ervoor kiest deel te nemen aan het privacyschildkader en het ministerie een klacht ontvangt dat deze maatschappij of dit bureau het kader zou hebben geschonden, dan neemt het ministerie de volgende stappen om het kader krachtig te handhaven.

([1]) http://www.transportation.gov/ai rconsumer/privacy-complaints

A. **Het geven van prioriteit aan het onderzoek van vermeende schendingen**

Het bureau voor handhaving betreffende de luchtvaart van het ministerie onderzoekt elke klacht waarin wordt gesteld dat het privacyschild is geschonden (waaronder klachten van Europese gegevensbeschermingsautoriteiten) en neemt handhavingsmaatregelen wanneer er bewijs is voor de schending. Daarnaast werkt het bureau voor handhaving betreffende de luchtvaart 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 privacyschildkader zijn gedaan.

Na ontvangst van een beschuldiging van schending van het privacyschildkader kan het bureau voor handhaving betreffende de luchtvaart van het ministerie als onderdeel van zijn onderzoek een reeks aan maatregelen nemen. Het kan bijvoorbeeld het privacybeleid van het reisbureau of de luchtvaartmaatschappij beoordelen, nadere informatie opvragen bij het bureau of de maatschappij 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 het privacyschild 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 het privacyschild.

B. **Aanpak van valse of misleidende verklaringen over het lidmaatschap**

Het ministerie blijft zich inspannen om schendingen van het privacyschild te onderzoeken, waaronder valse of misleidende verklaringen over het lidmaatschap van het privacyschildprogramma. We geven prioriteit aan verwijzingen van het ministerie van Handel inzake organisaties waarvan het ministerie vaststelt dat zij zich ten onrechte uitgeven als lid van het privacyschild of dat zij het keurmerk van het privacyschildkader zonder toestemming gebruiken.

Daarnaast merken we op dat indien in het kader van het privacybeleid van een organisatie wordt beloofd dat zij voldoet aan de materiële privacyschildbeginselen, het feit dat de organisatie zich niet bij het ministerie van Handel registreert of haar registratie daar niet verlengt, op zichzelf waarschijnlijk geen reden vormt om de organisatie te vrijwaren van de handhaving door het ministerie van Vervoer van deze toezegging.

C. **Toezicht op uitvoering en openbaarmaking van handhavingsbevelen inzake schendingen van het privacyschild**

Het bureau voor handhaving betreffende de luchtvaart 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 het privacyschildprogramma 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 het privacyschild 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 privacyschildzaken 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 privacyschild.

Ik hoop u hiermee voldoende te hebben geïnformeerd. Mocht u vragen hebben of meer informatie willen, dan kunt u altijd contact met mij opnemen.

Met vriendelijke groet,

Anthony R. Foxx

Minister van Vervoer

BIJLAGE VI

Brief van General Counsel Robert Litt
Office of the Director of National Intelligence

22 februari 2016

Dhr. Justin S. Antonipillai
Counselor
Amerikaans ministerie van Handel
1401 Constitution Ave., NW
Washington, DC 20230

Dhr. Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Geachte heren Antonipillai en Dean:

De afgelopen tweeënhalf jaar heeft de VS in het kader van de onderhandelingen over het EU-VS-privacyschild veel informatie verstrekt over de werking van de Amerikaanse inlichtingendiensten wat betreft hun activiteiten inzake het verzamelen van inlichtingen uit berichtenverkeer. Het ging onder meer om informatie over het toepasselijke rechtskader, het meerlagige toezicht op die activiteiten, de uitgebreide transparantie over deze activiteiten en de algemene waarborgen voor de privacy en burgerlijke vrijheden, om de Europese Commissie te helpen de adequaatheid te bepalen van deze waarborgen voor zover zij verband houden met de uitzondering op de privacyschildbeginselen op grond van de nationale veiligheid. In dit document wordt de verstrekte informatie samengevat.

I. PPD-28 EN HET UITVOEREN VAN ACTIVITEITEN IN HET KADER VAN INLICHTINGEN UIT BERICHTENVERKEER DOOR DE VS

De Amerikaanse inlichtingendiensten verzamelen buitenlandse inlichtingen op een nauwkeurig gecontroleerde wijze, in strikte overeenstemming met het Amerikaanse recht en onderworpen aan meerdere toezichtslagen, waarbij de nadruk ligt op belangrijke buitenlandse inlichtingen en nationale veiligheidsprioriteiten. Op het verzamelen van inlichtingen uit berichtenverkeer door de VS is een veelheid aan wetgeving en beleid van toepassing, waaronder de Amerikaanse grondwet, de Foreign Intelligence Surveillance Act (50 U.S.C. § 1801 e.v.) (hierna „FISA" genoemd), Executive Order (uitvoeringsbevel) 12333 en de uitvoeringsprocedures daarvan, presidentiële richtlijnen en talrijke procedures en richtlijnen die zijn goedgekeurd door de FISA Court en de Attorney General waarin aanvullende voorschriften zijn vastgesteld die het verzamelen, bewaren, gebruiken en verspreiden van buitenlandse inlichtingen beperken ([1]).

a) **PPD 28 overzicht**

In januari 2014 hield president Obama een toespraak waarin hij verscheidene hervormingen van de Amerikaanse activiteiten in het kader van inlichtingen uit berichtenverkeer aankondigde en vaardigde hij Presidential Policy Directive 28 (hierna „PPD-28" genoemd) uit die betrekking heeft op deze activiteiten ([2]). De president benadrukte dat de Amerikaanse activiteiten in het kader van inlichtingen uit berichtenverkeer niet alleen helpen ons land en onze vrijheden te beveiligen, maar ook de veiligheid en de vrijheden van andere landen helpen waarborgen, waaronder de EU-lidstaten, die vertrouwen op informatie van de Amerikaanse inlichtingendiensten om hun eigen burgers te beschermen.

In PPD-28 wordt een reeks beginselen en vereisten vastgesteld die van toepassing zijn op alle Amerikaanse activiteiten in het kader van inlichtingen uit berichtenverkeer en die gelden voor alle personen, ongeacht hun nationaliteit of de plaats waar zij zich bevinden. In de PPD-28 worden met name bepaalde vereisten vastgesteld voor procedures voor het verzamelen, bewaren en verspreiden van persoonsgegevens van niet-VS-burgers die zijn verkregen door middel van Amerikaanse inlichtingen uit berichtenverkeer. Deze vereisten worden verderop meer gedetailleerd beschreven, maar behelzen samengevat het volgende:

— in de PPD-28 wordt herhaald dat de VS alleen inlichtingen uit berichtenverkeer verzamelt voor zover dat is toegestaan bij wet, uitvoeringsbevel of andere presidentiële richtlijn.

([1]) Nadere informatie over buitenlandse inlichtingenactiviteiten van de VS wordt online gepubliceerd en is beschikbaar via *IC on the Record* (www.icontherecord.tumblr.com), de openbare website van het Office of the Director of National Intelligence (bureau van de directeur van het nationale inlichtingenwerk, hierna „ODNI" genoemd) die als doel heeft meer publieke zichtbaarheid te geven aan de inlichtingenactiviteiten van de overheid.

([2]) Beschikbaar op https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

— in PPD-28 worden procedures vastgesteld die moeten verzekeren dat activiteiten in het kader van inlichtingen uit berichtenverkeer uitsluitend worden uitgevoerd ter bevordering van rechtmatige en toegestane doeleinden in verband met nationale veiligheid.

— de PPD-28 schrijft ook voor dat bij het plannen van activiteiten voor de verzameling van inlichtingen uit berichtenverkeer rekening moet worden gehouden met privacy en burgerlijke vrijheden. De VS verzamelt met name geen inlichtingen om kritiek of afwijkende meningen te onderdrukken of te bemoeilijken, om personen te benadelen op basis van hun etniciteit, ras, geslacht, seksuele gerichtheid of religie of om een concurrerend handelsvoordeel te verlenen aan Amerikaanse bedrijven en bedrijfssectoren.

— in de PPD-28 is bepaald dat het verzamelen van inlichtingen uit berichtenverkeer zo gericht mogelijk moet plaatsvinden en dat bulksgewijs verzamelde inlichtingen uit berichtenverkeer uitsluitend voor bepaalde, specifiek opgesomde doeleinden kunnen worden gebruikt.

— de PPD-28 bepaalt dat de inlichtingendiensten procedures vaststellen die redelijkerwijs zijn opgezet om de verspreiding en de opslag van persoonsgegevens die door middel van activiteiten in het kader van inlichtingen uit berichtenverkeer zijn verzameld, te beperken en die met name bepaalde waarborgen die van toepassing zijn op de persoonsgegevens van Amerikanen, uitbreiden naar persoonsgegevens van niet-Amerikanen.

— voor overheidsinstanties zijn procedures ter uitvoering van PPD-28 vastgesteld en openbaar gemaakt.

De toepasselijkheid van de procedures en waarborgen die hierin zijn vastgesteld op het privacyschild, is duidelijk. Wanneer overeenkomstig het privacyschild, of via andere middelen, gegevens zijn overgedragen aan bedrijven in de Verenigde Staten, dan kunnen de Amerikaanse inlichtingendiensten die gegevens uitsluitend opvragen bij die bedrijven als het verzoek voldoet aan de FISA of wordt ingediend op grond van een van de wettelijke bepalingen van de National Security Letter, die hierna worden besproken ([1]). Bovendien zouden, zonder bevestiging of ontkenning van mediaverslagen waarin wordt gesteld dat de Amerikaanse inlichtingendiensten gegevens verzamelen van trans-Atlantische kabels, terwijl deze worden overgedragen naar de Verenigde Staten, de Amerikaanse inlichtingendiensten, mochten zij gegevens verzamelen via trans-Atlantische kabels, dan zouden zij dat doen onder toepassing van de beperkingen en waarborgen die hierin zijn vastgesteld, waaronder de vereisten van PPD-28.

b) **Beperkingen wat het verzamelen betreft**

In PPD-28 wordt een aantal belangrijke algemene beginselen vastgesteld die van toepassing zijn op het verzamelen van inlichtingen uit berichtenverkeer:

— het verzamelen van inlichtingen uit berichtenverkeer moet zijn toegestaan op grond van een wet of presidentiële goedkeuring en moet geschieden overeenkomstig de grondwet en de wetgeving.

— de privacy en de burgerlijke vrijheden moeten integrale overwegingen zijn bij de planning van activiteiten in het kader van inlichtingen uit berichtenverkeer.

— inlichtingen uit berichtenverkeer worden uitsluitend verzameld wanneer er een rechtmatig doeleinde is in het kader van buitenlandse inlichtingen of contra-inlichtingen.

— de Verenigde Staten verzamelen geen inlichtingen uit berichtenverkeer met het oog op de onderdrukking of bemoeilijking van kritiek of een afwijkende mening.

— de Verenigde Staten verzamelen geen inlichtingen uit berichtenverkeer om mensen te benadelen op basis van hun etniciteit, ras, geslacht, seksuele geaardheid of religie.

— de Verenigde Staten verzamelen geen inlichtingen uit berichtenverkeer om een concurrerend voordeel te verlenen aan Amerikaanse bedrijven of bedrijfssectoren.

— Amerikaanse activiteiten in het kader van inlichtingen uit berichtenverkeer moeten altijd zo gericht mogelijk plaatsvinden, rekening houdend met de beschikbaarheid van andere informatiebronnen. Dit houdt onder andere in dat, wanneer dat mogelijk is, activiteiten in het kader van de verzameling van inlichtingen uit berichtenverkeer gericht worden uitgevoerd en niet bulksgewijs.

Het vereiste dat activiteiten in het kader van inlichtingen uit berichtenverkeer „zo gericht mogelijk" moeten plaatsvinden, is van toepassing op de wijze waarop de inlichtingen uit berichtenverkeer worden verzameld en tevens op wat er

([1]) Regelgevende of wetshandhavingsinstanties kunnen informatie opvragen bij bedrijven voor onderzoeksdoeleinden in de Verenigde Staten overeenkomstig andere strafrechtelijke, civiele en regelgevende instanties die buiten de reikwijdte van dit overzicht vallen, dat is beperkt tot nationale veiligheidsinstanties.

daadwerkelijk wordt verzameld. Bij de beslissing om inlichtingen uit berichtenverkeer te gaan verzamelen, moeten de inlichtingendiensten bijvoorbeeld in overweging nemen of er andere informatie beschikbaar is, waaronder uit diplomatische of openbare bronnen, en de verzameling via deze bronnen prioriteit geven, indien dat passend en haalbaar is. Bovendien moeten onderdelen van de inlichtingendiensten,waar mogelijk, vereisen dat het verzamelen door middel van discriminanten (bv. specifieke voorzieningen, selectietermen en identificatoren) wordt gericht op specifieke doelwitten of onderwerpen van buitenlandse inlichtingen.

Het is belangrijk om de informatie die aan de Commissie wordt verstrekt als één geheel te beschouwen. Besluiten over wat „haalbaar" of „praktisch" is, worden niet overgelaten aan de beslissingsbevoegdheid van personen, maar zijn onderworpen aan beleidsmaatregelen die de instanties hebben vastgesteld op grond van PPD-28, en die openbaar zijn gemaakt, en aan andere hierin beschreven processen ([1]). Zoals in PPD-28 is bepaald, wordt onder het bulksgewijs verzamelen van inlichtingen uit berichtenverkeer verstaan: de verzameling die als gevolg van technische of operationele overwegingen wordt verkregen zonder het gebruik van discriminanten (bv. specifieke identificatoren, selectietermen enz.). In dit opzicht wordt in PPD-28 erkend dat onderdelen van de inlichtingendiensten in bepaalde omstandigheden inlichtingen uit berichtenverkeer bulksgewijs moeten verzamelen om nieuwe of opkomende dreigingen en andere informatie over de nationale veiligheid te identificeren die vaak verborgen is binnen het grote en complexe systeem van moderne wereldwijde communicatie. Tevens worden de zorgen op het gebied van privacy en burgerlijke vrijheden erkend die ontstaan bij het bulksgewijs verzamelen van inlichtingen uit berichtenverkeer. Daarom wordt de inlichtingendiensten in PPD-28 opgedragen alternatieven waarmee gerichte inlichtingen uit berichtenverkeer kunnen worden uitgevoerd voorrang te geven boven het bulksgewijs verzamelen van inlichtingen uit berichtenverkeer. Onderdelen van de inlichtingendiensten moeten derhalve, wanneer dat haalbaar is, gerichte activiteiten in het kader van het verzamelen van inlichtingen uit berichtenverkeer uitvoeren in plaats van activiteiten voor het bulksgewijs verzamelen van inlichtingen uit berichtenverkeer ([2]). Deze beginselen verzekeren dat de algemene regel niet wordt herroepen door de uitzondering voor bulksgewijs verzamelen.

Het concept „redelijkheid" is een ankerpunt in de Amerikaanse wetgeving. Het houdt in dat de onderdelen van de inlichtingendiensten niet elke theoretisch mogelijke maatregel hoeven te nemen, maar hun inspanningen ter bescherming van de rechtmatige belangen op het gebied van privacy en burgerlijke vrijheden in evenwicht moeten brengen met de praktische vereisten van activiteiten in het kader van inlichtingen uit berichtenverkeer. Ook hier zijn de beleidsmaatregelen van de instanties beschikbaar gemaakt en deze kunnen de verzekering bieden dat de term „redelijkerwijs ontworpen om de verspreiding en opslag van persoonsgegevens te beperken", de algemene regel niet ondermijnt.

PPD-28 voorziet er tevens in dat bulksgewijs verzamelde inlichtingen uit berichtenverkeer uitsluitend kunnen worden gebruikt voor zes doeleinden: opsporen en bestrijden van bepaalde activiteiten van buitenlandse mogendheden; contraterrorisme; bestrijding van wapendistributie; cyberveiligheid; opsporen en bestrijden van dreigingen tegen de Amerikaanse of geallieerde krijgsmacht; en de bestrijding van grensoverschrijdende criminele dreigingen, waaronder het ontwijken van sancties. De nationale veiligheidsadviseur van de president beoordeelt, in overleg met de Director for National Intelligence (directeur van het inlichtingenwerk, hierna „DNI" genoemd), jaarlijks het toegestane gebruik van bulksgewijs verzamelde inlichtingen uit berichtenverkeer om te zien of dit moeten worden gewijzigd. De DNI maakt deze lijst voor zover mogelijk en in overeenstemming met de nationale veiligheid openbaar beschikbaar. Dit biedt een belangrijke en transparante beperking van het gebruik van bulksgewijze verzameling van inlichtingen uit berichtenverkeer.

Daarnaast hebben de onderdelen van de inlichtingendiensten die PPD-28 hebben uitgevoerd bestaande analysepraktijken en normen voor het onderzoeken van niet-beoordeelde inlichtingen uit berichtenverkeer versterkt ([3]). Analisten moeten hun zoekopdrachten of andere zoektermen en -technieken zo vormgeven dat wordt verzekerd dat ze uitsluitend geschikt zijn om inlichtingen te identificeren die betrekking hebben op een geldige taak in het kader van buitenlandse inlichtingen of wetshandhaving. Hiervoor moeten onderdelen van de inlichtingendiensten zoekopdrachten over personen richten op de categorieën inlichtingen uit berichtenverkeer die het meest geschikt zin voor een vereiste in het kader van buitenlandse inlichtingen of wetshandhaving, om zo te voorkomen dat persoonsgegevens worden gebruikt die geen onderdeel vormen van vereisten in het kader van buitenlandse inlichtingen of wetshandhaving.

Er moet worden benadrukt dat eventuele bulksgewijze verzamelingsactiviteiten met betrekking tot internetcommunicatie die de Amerikaanse inlichtingendiensten door middel van inlichtingen uit berichtenverkeer uitvoeren, betrekking hebben op een klein deel van het internet. Daarnaast verzekert het gebruik van gerichte zoekopdrachten, zoals hiervoor beschreven, dat uitsluitend die onderdelen waarvan wordt aangenomen dat ze mogelijk van waarde zijn voor inlichtingen, ter onderzoek worden aangeboden aan analisten. Deze beperkingen zijn ingesteld om de privacy en burgerlijke vrijheden van eenieder te beschermen, ongeacht nationaliteit of verblijfplaats.

([1]) Beschikbaar op www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Deze procedures geven op een voor elk onderdeel van de inlichtingendiensten specifieke wijze uitvoering aan het concept van gerichte verzameling, zoals besproken in deze brief.

([2]) Om maar één voorbeeld aan te halen: in de procedures van de NSA waarmee PPD-28 wordt uitgevoerd, is bepaald dat „[w]anneer dat praktisch is, de verzameling plaatsvindt met behulp van een of meer selectietermen om de verzameling te richten op specifieke doelwitten van de buitenlandse inlichtingen (bv. een specifieke, bekende internationale terrorist of terroristische groepering) of specifieke onderwerpen van buitenlandse inlichtingen (bv. de verspreiding van massavernietigingswapens door een buitenlandse mogendheid of diens vertegenwoordigers).".

([3]) Beschikbaar op http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf

De Verenigde Staten hebben uitgebreide processen ingesteld om te verzekeren dat activiteiten in het kader van inlichtingen uit berichtenverkeer uitsluitend worden uitgevoerd ter bevordering van geschikte doeleinden op het gebied van de nationale veiligheid. Elk jaar stelt de president de hoogste prioriteiten van het land vast voor het verzamelen van buitenlandse inlichtingen, na een uitgebreid en formeel proces dat tussen de instanties plaatsvindt. De DNI is ervoor verantwoordelijk deze inlichtingenprioriteiten op te nemen in het nationaal kader voor inlichtingenprioriteiten, ofwel NIPF. PPD-28 heeft de processen tussen de instanties versterkt en verbeterd, om te verzekeren dat alle inlichtingenprioriteiten van de inlichtingendiensten worden beoordeeld en goedgekeurd door beleidsmakers op hoog niveau. Intelligence Community Directive 204 voorziet in nadere richtsnoeren over het NIPF en is in januari 2015 bijgewerkt om de vereisten van PPD-28 op te nemen ([1]). Hoewel het NIPF vertrouwelijk is, wordt informatie in verband met specifieke prioriteiten van de Amerikaanse buitenlandse inlichtingen jaarlijks opgenomen in de niet-vertrouwelijke *Worldwide Threat Assessment*, die ook beschikbaar is op de website van het ODNI.

De prioriteiten in het NIPF zijn redelijk algemeen geformuleerd. Ze omvatten onderwerpen als het onderzoeken van de mogelijkheden van ballistische en kernraketten door bepaalde buitenlandse opponenten, de gevolgen van corruptie door drugkartels en mensenrechtenschendingen in bepaalde landen. Ze zijn ook niet uitsluitend van toepassing op inlichtingen uit berichtenverkeer, maar op alle inlichtingenactiviteiten. De organisatie die verantwoordelijk is voor het vertalen van de prioriteiten in het NIPF naar de daadwerkelijke verzameling van inlichtingen uit berichtenverkeer is de National Signals Intelligence Committee (nationale commissie voor inlichtingen uit berichtenverkeer), oftewel SIGCOM. SIGCOM opereert onder toezicht van de directeur van het National Security Agency (NSA), die wordt aangewezen door uitvoeringsbevel 12333 als de „functioneel beheerder voor inlichtingen uit berichtenverkeer", verantwoordelijk voor het toezicht op en de coördinatie van inlichtingen uit berichtenverkeer binnen de inlichtingendiensten onder toezicht van de minister van Defensie en de DNI. SIGCOM heeft vertegenwoordigers uit alle onderdelen van de inlichtingendiensten en, nadat de Verenigde Staten PPD-28 volledig hebben uitgevoerd, zal deze commissie tevens vertegenwoordigers hebben uit andere ministeries en instanties die beleidsbelang hebben bij inlichtingen uit berichtenverkeer.

Alle Amerikaanse ministeries en instanties die afnemers zijn van buitenlandse inlichtingen, dienen hun verzoeken voor verzameling in bij SIGCOM. SIGCOM beoordeelt deze verzoeken, waarborgt dat deze overeenstemmen met het NIPF en wijst prioriteiten toe aan de hand van criteria zoals:

— kunnen inlichtingen uit berichtenverkeer in dit geval nuttige informatie bieden of zijn er betere of kostenefficiëntere informatiebronnen om dit vereiste aan te pakken, zoals afbeeldingen of informatie uit open bronnen?

— hoe cruciaal is deze informatie? Als deze een hoge prioriteit heeft in het NIPF, heeft deze meestal ook een hoge prioriteit in het kader van inlichtingen uit berichtenverkeer.

— welk soort inlichtingen uit berichtenverkeer kan worden gebruikt?

— wordt er zo gericht mogelijk verzameld? Zijn er beperkingen, bijvoorbeeld in tijd of locatie?

In het proces voor de vereisten van Amerikaanse inlichtingen uit berichtenverkeer moet tevens expliciet aandacht worden besteed aan andere factoren, namelijk:

— is het doelwit van de verzameling of de methodologie die voor het verzamelen wordt gebruikt, bijzonder gevoelig? Als dat het geval is, dan moet dit worden beoordeeld door senior beleidsmakers.

— vormt de verzameling een ongeoorloofd risico voor de privacy en burgerlijke vrijheden, ongeacht de nationaliteit?

— zijn er aanvullende waarborgen op het gebied van verspreiding en opslag noodzakelijk om de privacy of belangen in het kader van de nationale veiligheid te beschermen?

Tot slot bekijkt speciaal opgeleid NSA-personeel, aan het eind van het proces, de door SIGCOM en het onderzoek gevalideerde prioriteiten en stelt specifieke selectietermen vast, zoals telefoonnummers of e-mailadressen, waarvan wordt gedacht dat hiermee buitenlandse inlichtingen kunnen worden verzameld in het kader van deze prioriteiten. Elke selectieterm moet worden beoordeeld en goedgekeurd voordat deze wordt ingevoerd in de verzamelsystemen van de NSA. En zelfs dan is het de vraag of en wanneer de daadwerkelijke verzameling plaatsvindt afhankelijk van aanvullende overwegingen, zoals de beschikbaarheid van passende bronnen voor de verzameling. Dit proces waarborgt dat het verzamelen van inlichtingen uit berichtenverkeer door de VS een afspiegeling vormt van geldige en belangrijke behoeften

([1]) Beschikbaar op http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf

op het gebied van buitenlandse inlichtingen. Daarnaast moeten de NSA en andere instanties, wanneer de verzameling wordt uitgevoerd overeenkomstig de FISA, zich natuurlijk houden aan aanvullende beperkingen die zijn goedgekeurd door de Foreign Intelligence Surveillance Court. Kortom, de NSA noch een andere Amerikaanse inlichtingeninstantie besluit zelfstandig wat er wordt verzameld.

Dit proces verzekert in het algemeen dat alle Amerikaanse inlichtingenprioriteiten worden vastgesteld door senior beleidsmakers die het beste in staat zijn om de vereisten in het kader van de buitenlandse inlichtingen van de VS te identificeren, en dat deze beleidsmakers niet alleen rekening houden met de mogelijke waarde van de verzamelde inlichtingen, maar ook met de risico's die samenhangen met de verzameling, waaronder risico's in het kader van privacy, nationale economische belangen en buitenlandse betrekkingen.

Met betrekking tot gegevens die naar de Verenigde Staten worden overgebracht overeenkomstig het privacyschild, kunnen de Verenigde Staten weliswaar geen specifieke inlichtingenmethoden of -activiteiten bevestigen of ontkennen, maar zijn de vereisten van PPD-28 van toepassing op alle activiteiten in het kader van inlichtingen uit berichtenverkeer die de Verenigde Staten uitvoeren, ongeacht de soort of de bron van de gegevens die worden verzameld. Bovendien zijn de beperkingen en waarborgen die van toepassing zijn op de verzameling van inlichtingen uit berichtenverkeer, ook van toepassing op inlichtingen uit berichtenverkeer die worden verzameld voor elk toegestaan gebruik, waaronder zowel buitenlandse betrekkingen als nationale veiligheidsdoelstellingen.

De hiervoor besproken procedures tonen aan dat er veel waarde wordt gehecht aan het voorkomen van de willekeurige en ongedifferentieerde verzameling van inlichtingen uit berichtenverkeer, en aan de uitvoering, vanuit onze hoogste regeringsniveaus, van het beginsel van redelijkheid. PPD-28 en uitvoeringsprocedures van de instanties verduidelijken nieuwe en bestaande beperkingen van en beschrijven specifieker het doeleinde waarvoor de Verenigde Staten inlichtingen uit berichtenverkeer verzamelen en gebruiken. Deze procedures moeten verzekeren dat activiteiten in het kader van inlichtingen uit berichtenverkeer uitsluitend worden uitgevoerd om rechtmatige doelstellingen op het gebied van buitenlandse inlichtingen te bevorderen.

c) **Beperkingen aan de opslag en verspreiding**

In sectie 4 van PPD-28 wordt verplicht dat elk onderdeel van de inlichtingendiensten expliciete beperkingen invoert voor de opslag en verspreiding van persoonsgegevens over niet-Amerikanen die zijn verzameld met behulp van inlichtingen uit berichtenverkeer, die vergelijkbaar zijn met de beperkingen voor Amerikanen. Deze voorschriften zijn opgenomen in procedures voor elke inlichtingendienst die zijn vrijgegeven in februari 2015 en openbaar beschikbaar zijn. Om in aanmerking te komen voor opslag of verspreiding als buitenlandse inlichtingen, moeten persoonsgegevens verband houden met een toegestaan inlichtingenvereiste, zoals vastgesteld in de NIPF-procedure die hiervoor is beschreven; moet redelijkerwijs worden aangenomen dat zij het bewijs vormen van een misdrijf; of moeten zij voldoen aan een van de andere normen voor opslag van Amerikaanse persoonsgegevens, zoals vermeld in sectie 2.3 van uitvoeringsbevel 12333.

Informatie waarvoor een dergelijk vaststelling niet is gemaakt, mag niet worden opgeslagen voor een periode langer dan vijf jaar, tenzij de DNI expliciet vaststelt dat verlengde opslag noodzakelijk is in het belang van de nationale veiligheid van de Verenigde Staten. Derhalve moeten onderdelen van de inlichtingendiensten persoonsgegevens van niet-Amerikanen die zijn verzameld met behulp van inlichtingen uit berichtenverkeer vijf jaar na de verzameling verwijderen, tenzij bijvoorbeeld is vastgesteld dat de gegevens relevant zijn voor een toegestaan vereiste in het kader van buitenlandse inlichtingen of als de DNI bepaalt, na beoordeling van de standpunten van de functionarissen voor de bescherming van burgerlijke vrijheden van het ODNI en van de instellingen, dat langere opslag in het belang is van de nationale veiligheid.

Daarnaast wordt in alle beleidsmaatregelen van instanties die PPD-28 ten uitvoer leggen, expliciet vereist dat gegevens over een persoon niet mogen worden verspreid uitsluitend omdat een betrokkene geen Amerikaan is, en heeft het ODNI een richtlijn uitgevaardigd voor alle onderdelen van de inlichtingendiensten ([1]) waarin dit vereiste is opgenomen. Personeel van de inlichtingendiensten moet specifiek rekening houden met de privacybelangen van niet-Amerikanen wanneer zij inlichtingenrapporten opstellen en verspreiden. Inlichtingen uit berichtenverkeer worden met name met betrekking tot de routineactiviteiten van een buitenlandse persoon niet beschouwd als buitenlandse inlichtingen die kunnen worden verspreid of permanent bewaard op grond van dat enkele feit, tenzij dat is afgestemd op een toegestaan vereiste in het kader van buitenlandse inlichtingen. Hiermee wordt dit erkend als een belangrijke beperking en dit is een reactie op de zorgen van de Europese Commissie over de reikwijdte van de definitie van buitenlandse inlichtingen, zoals vastgesteld in uitvoeringsbevel 12333.

([1]) Intelligence Community Directive (ICD) 203, beschikbaar op http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf

d) **Naleving en toezicht**

Het Amerikaanse systeem van toezicht op buitenlandse inlichtingen voorziet in strikt en meerlagig toezicht om de naleving van toepasselijke wetgeving en procedures te waarborgen, waaronder die welke betrekking hebben op het verzamelen, opslaan en verspreiden van gegevens over niet-Amerikanen die zijn verkregen door middel van inlichtingen uit berichtenverkeer, zoals beschreven in PPD-28. Het gaat onder meer om de volgende gebieden:

— bij de inlichtingendiensten zijn honderden mensen werkzaam als toezichthoudend personeel. Alleen al de NSA heeft 300 mensen in dienst die zich toeleggen op naleving, en de andere onderdelen hebben ook toezichtsafdelingen. Bovendien biedt het ministerie van Justitie uitgebreid toezicht op de inlichtingenactiviteiten, en vindt er tevens vanuit het ministerie van Defensie toezicht plaats.

— elk onderdeel van de inlichtingendiensten heeft zijn eigen Office of the Inspector General (bureau van de inspecteur-generaal) dat verantwoordelijk is voor, onder andere, het toezicht op de buitenlandse inlichtingenactiviteiten. Een inspecteur-generaal is wettelijk onafhankelijk, heeft een ruime bevoegdheid om onderzoek, audits en evaluaties van programma's uit te voeren, onder meer op het gebied van fraude en misbruik of schending van de wet, en kan corrigerende maatregelen voorstellen. Hoewel aanbevelingen van een inspecteur-generaal niet bindend zijn, worden de verslagen van inspecteurs-generaal vaak openbaar gemaakt en zijn zij in elk geval beschikbaar voor het Congres. Dit omvat tevens follow-upverslagen voor het geval waarin correctieve maatregelen die zijn aanbevolen in eerdere verslagen, nog niet zijn voltooid. Het Congres wordt derhalve geïnformeerd over de niet-naleving en kan druk uitoefenen, onder meer door middel van de begroting, om een correctieve maatregel te bewerkstelligen. Een aantal rapporten van inspecteurs-generaal over inlichtingenprogramma's zijn openbaar gemaakt ([1]).

— het Civil Liberties and Privacy Office (bureau voor burgerlijke vrijheden en privacy, hierna „CLPO" genoemd) van het ODNI is belast met het waarborgen dat de inlichtingendiensten zodanig opereren dat de nationale veiligheid wordt bevorderd, terwijl de burgerlijke vrijheden en privacyrechten worden beschermd ([2]). Andere onderdelen van de inlichtingendiensten hebben hun eigen privacyfunctionarissen.

— de Privacy and Civil Liberties Oversight Board (raad van toezicht op de privacy en de burgerlijke vrijheden, hierna „PCLOB" genoemd) is een onafhankelijk orgaan dat bij wet is opgericht en is belast met de analyse en beoordeling van programma's en beleid in het kader van contra-terrorisme, waaronder het gebruik van inlichtingen uit berichtenverkeer, om te waarborgen dat deze de privacy en burgerlijke vrijheden toereikend beschermen. Deze raad heeft meerdere openbare verslagen over inlichtingenactiviteiten opgesteld.

— zoals hierna in meer detail zal worden besproken, is het Foreign Intelligence Surveilance Court, een rechtbank die bestaat uit onafhankelijke federale rechters, verantwoordelijk voor het toezicht op en de naleving van activiteiten in het kader van het verzamelen van inlichtingen uit berichtenverkeer overeenkomstig de FISA.

— tot slot heeft het Congres van de Verenigde Staten, met name de inlichtingen- en rechterlijke commissies van het Huis van afgevaardigden en de Senaat, aanzienlijke verantwoordelijkheden voor het toezicht op alle buitenlandse inlichtingenactiviteiten van de Verenigde Staten, met inbegrip van inlichtingen uit berichtenverkeer van de Verenigde Staten.

Afgezien van deze formele toezichtsmechanismen hebben de inlichtingendiensten meerdere mechanismen ingevoerd om te waarborgen dat de inlichtingendiensten voldoen aan de verzamelingsbeperkingen die hiervoor worden beschreven. Bijvoorbeeld:

— kabinetsmedewerkers moeten hun vereisten inzake inlichtingen uit berichtenverkeer elk jaar valideren.

— de NSA controleert doelwitten van inlichtingen uit berichtenverkeer gedurende het gehele verzamelproces om vast te stellen of ze daadwerkelijk waardevolle buitenlandse inlichtingen opleveren die overeenkomen met de prioriteiten, en stopt de verzameling bij doelwitten waarbij daar geen sprake van is. Aanvullende procedures verzekeren dat de selectietermen periodiek worden herzien.

([1]) Zie bv., U.S. Department of Justice Inspector General Report „A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008" (september 2012), beschikbaar op https://oig.justice.gov/reports/2016/o1601a.pdf

([2]) Zie www.dni.gov/clpo

— op basis van een aanbeveling van een onafhankelijke herzieningsgroep die wordt benoemd door president Obama, heeft de directeur van de DNI een nieuw mechanisme ingesteld om toezicht te houden op de verzameling en verspreiden van inlichtingen uit berichtenverkeer die bijzonder gevoelig zijn als gevolg van de aard van het doelwit of de verzamelmethoden, om te verzekeren dat deze consistent is met de vaststellingen van beleidsmakers.

— tot slot voert het bureau van de directeur van de nationale inlichtingendienst jaarlijks een herziening uit van de toewijzing van middelen van de inlichtingendiensten ten opzichte van de NIPF-prioriteiten en de inlichtingenmissie als geheel. Deze herziening omvat beoordelingen van de waarde van alle soorten van inlichtingenverzameling, waaronder inlichtingen uit berichtenverkeer, en kijkt zowel terug (hoe succesvol waren de inlichtingendiensten bij het bereiken van hun doelstellingen?) als vooruit (wat hebben de inlichtingendiensten in de toekomst nodig?) Zo wordt verzekerd dat bronnen van inlichtingen uit berichtenverkeer worden toegepast op de belangrijkste nationale prioriteiten.

Zoals blijkt uit dit uitgebreide overzicht, beslissen de inlichtingendiensten niet zelfstandig over welke gesprekken zij afluisteren, proberen zij niet alles te verzamelen en handelen zij niet zonder enige vorm van toezicht. De activiteiten zijn voornamelijk gericht op door beleidsmakers vastgestelde prioriteiten, waarbij een proces wordt gevolgd dat rekening houdt met input vanuit de gehele overheid en waarop toezicht wordt gehouden zowel binnen de NSA als door het ODNI, het ministerie van Justitie en het ministerie van Defensie.

PPD-28 bevat tevens vele andere bepalingen die waarborgen dat persoonsgegevens die zijn verzameld in het kader van inlichtingen uit berichtenverkeer, worden beschermd, ongeacht de nationaliteit. Zo wordt er in PPD-28 bijvoorbeeld voorzien in gegevensbeveiliging, toegang en kwaliteitsprocedures om persoonsgegevens te beschermen die door middel van inlichtingen uit berichtenverkeer zijn verzameld, en wordt voorzien in verplichte opleiding om te waarborgen dat het personeel de verantwoordelijkheid om persoonsgegevens, ongeacht nationaliteit, te beschermen, begrijpt. PPD-28 voorziet ook in aanvullende toezichts- en nalevingsmechanismen. Deze mechanismen bestaan uit periodieke audits en beoordelingen door de bevoegde toezichts- en nalevingsfunctionarissen van de praktijken voor de bescherming van persoonsgegevens die deel uitmaken van inlichtingen uit berichtenverkeer. De beoordelingen moeten tevens onderzoeken of de instanties de procedures voor de bescherming van dergelijke informatie naleven.

Daarnaast is in PPD-28 vastgelegd dat omvangrijke nalevingsproblemen met betrekking tot niet-Amerikanen in de hogere overheidsniveaus worden aangepakt. Mocht er zich een omvangrijk nalevingsprobleem voordoen met betrekking tot persoonsgegevens van een persoon die zijn verzameld als gevolg van activiteiten in het kader van inlichtingen uit berichtenverkeer, dan moet dit probleem, in aanvulling op eventuele bestaande rapportagevereisten, direct worden gemeld bij de DNI. Als het probleem betrekking heeft op een niet-Amerikaanse persoon, bepaalt de DNI, in overleg met de minister van Buitenlandse Zaken en het hoofd van het desbetreffende onderdeel van de inlichtingendiensten, of er stappen moeten worden genomen om de relevante buitenlandse overheid op de hoogte te stellen, in overeenstemming met de bescherming van bronnen en methoden en van Amerikaans personeel. Bovendien heeft de minister van Buitenlandse Zaken, zoals vastgesteld in PPD-28, een senior ambtenaar, Under Secretary Catherine Novelli, aangesteld als contactpunt voor buitenlandse overheden die problemen willen aankaarten in verband met de activiteiten in het kader van inlichtingen uit berichtenverkeer van de Verenigde Staten. Deze betrokkenheid op hoog niveau is een voorbeeld van de inspanningen die de Amerikaanse overheid in de laatste paar jaar heeft gedaan om vertrouwen te scheppen voor de vele en overlappende privacybeschermingen die gelden voor gegevens van Amerikanen en niet-Amerikanen.

e) **Samenvatting**

De processen van de Verenigde Staten voor het verzamelen, opslaan en verspreiden van buitenlandse inlichtingen biedt belangrijke privacywaarborgen voor de persoonlijke gegevens van iedereen, ongeacht nationaliteit. Deze processen verzekeren in het bijzonder dat onze inlichtingendiensten zich richten op hun nationale veiligheidsmissie, zoals toegestaan door de toepasselijke wetgeving, uitvoeringsbevelen en presidentiële richtlijnen; gegevens beschermen tegen onbevoegde toegang, onbevoegd gebruik en onbevoegde openbaarmaking; en hun activiteiten uitvoeren overeenkomstig meerdere lagen van herziening en toezicht, waaronder door toezichtsommissies van het Congres. PPD-28 en de uitvoeringsprocedures daarvan geven onze inspanningen weer om bepaalde minimaliserings- en andere aanzienlijke beginselen op het gebied van gegevensbescherming uit te breiden naar de persoonsgegevens van eenieder, ongeacht nationaliteit. Op persoonsgegevens die worden verkregen door middel van de Amerikaanse verzameling van inlichtingen uit berichtenverkeer zijn de beginselen en vereisten van de Amerikaanse wetgeving en presidentiële sturing van toepassing, waaronder de in PPD-28 vastgestelde beschermingen. Deze beginselen en vereisten verzekeren dat iedereen met waardigheid en respect wordt behandeld, ongeacht nationaliteit of verblijfplaats, en erkennen dat eenieder rechtmatige privacybelangen heeft bij de verwerking van zijn persoonsgegevens.

II. FOREIGN INTELLIGENCE SURVEILLANCE ACT — SECTIE 702

Verzameling op grond van sectie 702 van de Foreign Surveillance Act ([1]) gebeurt niet op „grote schaal en ongedifferentieerd", maar is precies gericht op de verzameling van buitenlandse inlichtingen afkomstig van afzonderlijk geïdentificeerde rechtmatige doelwitten, wordt duidelijk toegestaan door expliciete wettelijke machtiging; en is onderworpen aan zowel onafhankelijk juridisch toezicht als omvangrijke herziening en toezicht binnen de uitvoerende macht en het Congres. Verzameling op grond van sectie 702 wordt beschouwd als inlichtingen uit berichtenverkeer, waarop de vereisten van PPD-28 van toepassing zijn ([2]).

Verzameling op grond van sectie 702 is een van de meest waardevolle bronnen van inlichtingen ter bescherming van zowel de Verenigde Staten als onze Europese partners. Uitgebreide informatie over de werking van en het toezicht op sectie 702 is openbaar beschikbaar. Er zijn vele gerechtsdocumenten, gerechtelijke besluiten en toezichtsverslagen in verband met het programma openbaar gemaakt en vrijgegeven op de website voor openbare bekendmaking van het ODNI: www.icontherecord.tumblr.com. Bovendien is sectie 702 uitgebreid geanalyseerd door het PCLOB, in een verslag dat beschikbaar is op https://www.pclob.gov/library/702-Report.pdf ([3]).

Sectie 702 is aangenomen als onderdeel van de FISA Amendments Act van 2008 ([4]), na uitgebreide openbare besprekingen in het Congres. Hierin wordt het verwerven van buitenlandse inlichtingen toegestaan door middel van het focussen op niet-Amerikaanse personen buiten de Verenigde Staten, met de gedwongen ondersteuning van Amerikaanse dienstverleners op het gebied van elektronische communicatie. In sectie 702 wordt de Attorney General en de DNI, twee functionarissen op kabinetsniveau die door de president worden benoemd en worden bevestigd door de Senaat, de bevoegdheid verleend om jaarlijkse certificaten te verstrekken aan de FISA-rechtbank ([5]). Deze certificaten identificeren specifieke categorieën buitenlandse inlichtingen die moeten worden verzameld, zoals inlichtingen over contra-terrorisme of massavernietigingswapens, die moeten vallen in een van de categorieën van buitenlandse inlichtingen die zijn gedefinieerd in de FISA ([6]). Zoals het PCLOB opmerkte „[s]taan deze beperkingen *niet* het onbeperkt verzamelen van informatie over buitenlanders toe" ([7]).

De certificeringen zijn ook vereist om de procedures met betrekking tot „gerichtheid" en „minimalisering" op te nemen, die moeten worden beoordeeld en goedgekeurd door de FISA-rechtbank ([8]). De gerichtheidsprocedures zijn ontworpen om te waarborgen dat de verzameling uitsluitend plaatsvindt zoals wettelijk is toegestaan en valt binnen de reikwijdte van de certificeringen; de minimaliseringsprocedures zijn ontworpen om de verwerving, verspreiding en opslag van informatie over Amerikaanse personen te beperken, maar bevatten tevens bepalingen die uitgebreide bescherming bieden aan de gegevens over niet-Amerikanen, zoals hierna wordt beschreven. Bovendien is, zoals hiervoor is beschreven, in PPD-28 door de president bepaald dat de inlichtingendiensten aanvullende waarborgen moeten verstrekken voor persoonsgegevens van niet-Amerikanen en dat deze waarborgen van toepassing zijn op gegevens die zijn verzameld op grond van sectie 702.

Zodra de rechtbank de gerichtheids- en minimaliseringsprocedures goedkeurt, wordt verzameling op grond van sectie 702 niet gezien als bulksgewijs of ongedifferentieerd, maar „is deze volledig gericht op specifieke personen over wie een geïndividualiseerd besluit is genomen", zoals het PCLOB verklaarde ([9]). De verzameling wordt gericht door middel van het gebruik van afzonderlijke selectoren, zoals e-mailadressen of telefoonnummers, waarvan medewerkers van de Amerikaanse inlichtingendiensten hebben vastgesteld dat deze waarschijnlijk worden gebruikt om buitenlandse

([1]) 50 U.S.C. § 1881a.

([2]) De Verenigde Staten kunnen ook gerechtelijke bevelen verkrijgen overeenkomstig de andere bepalingen van de FISA voor de productie van gegevens, waaronder gegevens die worden overgedragen in het kader van het privacyschild. Zie 50 U.S.C. § 1801 e.v. Titels I en III van de FISA, waarin respectievelijk elektronische surveillance en fysieke zoekopdrachten worden toegestaan, vereisen altijd een gerechtelijk bevel (uitgezonderd in geval van nood) evenals gerede aanleiding om aan te nemen dat het doelwit een buitenlandse mogendheid is of een agent van een buitenlandse mogendheid. In titel IV van FISA wordt het gebruik van nummerregistratie en traceerapparatuur toegestaan, overeenkomstig een gerechtelijk bevel (uitgezonderd in geval van nood) in toelaatbare onderzoeken betreffende buitenlandse inlichtingen, contra-inlichtingen of contra-terrorisme. In titel V van de FISA wordt de FBI toegestaan om, overeenkomstig een gerechtelijk bevel (uitgezonderd in geval van nood) bedrijfsgegevens op te vragen die relevant zijn voor een toelaatbaar onderzoek betreffende buitenlandse inlichtingen, contra-inlichtingen of contra-terrorisme. Zoals hierna wordt besproken, wordt in de USA FREEDOM Act het gebruik van FISA-bevelen inzake nummerregistratie en traceerapparatuur verboden voor bulksgewijze verzameling en wordt een vereiste ingesteld van een „specifieke selectieterm" om te verzekeren dat deze bevoegdheden gericht worden gebruikt.

([3]) Privacy and Civil Liberties Board, „Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (2 juli 2014) (hierna „PCLOB-verslag" genoemd).

([4]) Zie Pub. L. No. 110-261, 122 Stat. 2436 (2008).

([5]) Zie 50 U.S.C. § 1881a(a) en (b).

([6]) Zie id. § 1801(e).

([7]) Zie het PCLOB-verslag, punt 99.

([8]) Zie 50 U.S.C. § 1881a(d) en (e).

([9]) Zie het PCLOB-verslag, punt 111.

inlichtingen te communiceren van het type waarop de bij de rechtbank ingediende certificering van toepassing is ([1]). De basis voor de selectie van het doelwit moet schriftelijk worden vastgelegd en de documentatie voor elke selector wordt vervolgens beoordeeld door het ministerie van Justitie ([2]). De Amerikaanse overheid heeft informatie vrijgegeven waaruit blijkt dat er in 2014 ongeveer 90 000 personen werden onderzocht op grond van sectie 702, slechts een minuscule hoeveelheid van de meer dan drie miljard internetgebruikers wereldwijd ([3]).

Informatie die is verzameld op grond van sectie 702 is onderworpen aan door de rechtbank goedgekeurde minimaliseringsprocedures, waarmee bescherming wordt geboden aan zowel niet-Amerikanen als Amerikanen, en die openbaar zijn gemaakt ([4]). Communicatie die bijvoorbeeld is verkregen op grond van sectie 702, ongeacht of deze afkomstig is van Amerikanen of niet-Amerikanen, wordt opgeslagen in databanken met een strikte toegangscontrole. Deze communicatie mag alleen worden bekeken door medewerkers van de inlichtingendiensten die zijn opgeleid op het gebied van minimaliseringsprocedures in het kader van privacybescherming en die specifiek toestemming hebben gekregen voor die toegang om de functies uit te oefenen waartoe zij gemachtigd zijn ([5]). Het gebruik van de gegevens is beperkt tot de identificatie van buitenlandse inlichtingen of het bestaan van een misdrijf ([6]). Op grond van PPD-28 mag deze informatie uitsluitend worden verspreid als er een geldig doeleinde in het kader van buitenlandse inlichtingen of wetshandhaving bestaat; het enkele feit dat een partij bij de communicatie niet Amerikaans is, is onvoldoende ([7]). In de minimaliseringsprocedures en PPD-28 zijn ook beperkingen vastgesteld over hoe lang gegevens die zijn verzameld op grond van sectie 702, mogen worden bewaard ([8]).

Het toezicht op sectie 702 is uitgebreid en wordt uitgevoerd door alle drie de machten van onze overheid. Instanties die de wetgeving uitvoeren, beschikken over meerdere niveaus van interne beoordeling, waaronder door onafhankelijke inspecteurs-generaal, en technologische controles over toegang tot de gegevens. Het ministerie van Justitie en het bureau van de directeur van de nationale inlichtingendienst beoordelen en onderzoeken het gebruik van sectie 702 om de naleving met wettelijke voorschriften te verifiëren. Instanties hebben ook een onafhankelijke verplichting om mogelijke incidenten betreffende niet-naleving te rapporteren. Deze incidenten worden onderzocht en alle nalevingsincidenten worden gerapporteerd aan het Foreign Intelligence Surveillance Court, het Intelligence Oversight Board van de president, en het Congres en worden op passende wijze verholpen ([9]). Tot op heden hebben er geen incidenten of bewuste pogingen plaatsgevonden om de wetgeving te schenden of wettelijke vereisten te omzeilen ([10]).

De FISA-rechtbank speelt een belangrijke rol bij de uitvoering van sectie 702. Deze rechtbank bestaat uit onafhankelijke federale rechters die gedurende een termijn van zeven jaar zitting hebben in de FISA-rechtbank, maar die, net als alle federale rechters, voor het leven als rechter zijn benoemd. Zoals hiervoor is opgemerkt, moet deze rechtbank de jaarlijkse certificeringen en de gerichtheids- en minimaliseringsprocedures beoordelen op de naleving van de wet. Daarnaast is de overheid, zoals ook hiervoor al is opgemerkt, verplicht de rechtbank direct in kennis te stellen van nalevingsproblemen ([11]). Er zijn meerdere adviezen van de rechtbank openbaar gemaakt en vrijgegeven waaruit blijkt hoe nauwkeurig de onderzoeken plaatsvinden en hoe onafhankelijk de rechtbank functioneert in deze incidenten.

De veeleisende processen van de rechtbank zijn beschreven door de voormalige president van de rechtbank in een brief aan het Congres die openbaar is gemaakt ([12]). En als gevolg van de USA FREEDOM Act is de rechtbank, zoals hierna wordt beschreven, nu uitdrukkelijk bevoegd om een externe advocaat te benoemen als onafhankelijke pleitbezorger in het kader van de privacy in zaken waar nieuwe of belangrijke juridische kwesties aan de orde komen ([13]). Deze mate van betrokkenheid door de onafhankelijke rechterlijke macht van een land bij activiteiten in het kader van buitenlandse inlichtingen gericht op personen die geen burger zijn van dat land noch zich in dat land bevinden, is ongebruikelijk, zo niet ongekend, en helpt te waarborgen dat de verzameling in het kader van sectie 702 plaatsvindt binnen de toepasselijke juridische beperkingen.

([1]) Id.

([2]) Id. punt 8; 50 U.S.C. § 1881a(l); Zie *ook* NSA Director of Civil Liberties and Privacy Report, „NSA's Implementation of Foreign Intelligence Surveillance Act Section 702" (hierna het „NSA Report" genoemd) punt 4, beschikbaar op http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties

([3]) Director of National Intelligence 2014 Transparency Report, beschikbaar op http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014

([4]) De minimaliseringsprocedures zijn beschikbaar op: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf („NSA Minimization Procedures"); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; en http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf

([5]) Zie NSA-verslag, punt 4.

([6]) Zie bv. NSA Minimization Procedures, punt 6.

([7]) Intelligence Agency PPD-28 procedures beschikbaar op http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties

([8]) Zie NSA Minimization Procedures; PPD-28, sectie 4.

([9]) Zie 50 U.S.C. § 1881(l); zie ook het PCLOB-verslag, punten 66-76.

([10]) Zie Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, punten 2-3, beschikbaar op http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf

([11]) Rule 13 van de Foreign Intelligence Surveillance Court Rules of Procedures, beschikbaar op http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf

([12]) 29 juli 2013, brief van de edelachtbare Reggie B. Walton aan de edelachtbare Patrick J. Leahy, beschikbaar op http://fas.org/irp/news/2013/07/fisc-leahy.pdf

([13]) Zie sectie 401 van de USA FREEDOM Act, P.L. 114-23.

Het Congres oefent toezicht uit op grond van wettelijk vereiste verslagen aan de inlichtingen- en rechterlijke commissies, en regelmatige mededelingen en hoorzittingen. Deze omvatten een halfjaarlijks verslag van de Attorney General waarin de toepassing van sectie 702 en eventuele nalevingsincidenten worden beschreven ([1]); en een afzonderlijke halfjaarlijkse beoordeling van de Attorney General en DNI waarin de naleving van de procedures voor het specificeren van het doelwit en de minimaliseringsprocedures wordt gedocumenteerd, inclusief de naleving van de procedures die ervoor moeten zorgen dat de verzameling een geldig doel op het gebied van buitenlandse inlichtingen dient ([2]); en een jaarverslag afkomstig van de hoofden van inlichtingenonderdelen, met de certificering dat de verzameling op grond van sectie 702 nog steeds buitenlandse inlichtingen oplevert ([3]).

Kortom, de verzameling op grond van sectie 702 is wettelijk toegestaan; is onderworpen aan meerdere beoordelingsniveaus, rechterlijke controle en toezicht; en wordt, zoals de FISA-rechtbank verklaarde in een recentelijk openbaar gemaakt advies „niet bulksgewijs of op ongedifferentieerde manier uitgevoerd", maar „door middel van.. discrete gerichtheidsbesluiten voor afzonderlijke [communicatie]faciliteiten" ([4]).

III. USA FREEDOM ACT

De USA FREEDOM Act, die in juni 2015 in werking is getreden, heeft de Amerikaanse surveillance- en andere nationale veiligheidsinstanties aanzienlijk gewijzigd en de publieke transparantie over het gebruik van deze instanties en over beslissingen van de FISA-rechtbank verhoogd, zoals hierna wordt toegelicht ([5]). Deze wet verzekert dat onze professionals op het gebied van inlichtingen en wetshandhaving beschikken over de benodigde bevoegdheden om het land te beschermen, terwijl voorts wordt gewaarborgd dat de privacy van personen op passende wijze wordt beschermd wanneer van deze bevoegdheden gebruik wordt gemaakt. De wet verbetert de privacy en burgerlijke vrijheden en verhoogt de transparantie.

De wet verbiedt het bulksgewijs verzamelen van gegevens, zowel van Amerikanen als van niet-Amerikanen, op grond van verschillende bepalingen in de FISA of door middel van het gebruik van National Security Letters, een vorm van wettelijk toegestane administratieve dagvaardingen ([6]). Dit verbod omvat specifiek telefonische metagegevens die verband houden met gesprekken tussen personen binnen en buiten de Verenigde Staten en omvat tevens de verzameling van informatie in het kader van het privacyschild op grond van deze bevoegdheden. In de wet wordt verplicht dat de overheid een verzoek om gegevens op grond van deze bevoegdheden baseert op een „specifieke selectieterm", een term die een persoon, account, adres of persoonlijk apparaat specifiek identificeert op een manier die de omvang van de gewenste informatie zo ver als redelijk haalbaar is, beperkt ([7]). Zo wordt verder gewaarborgd dat de verzameling van informatie voor inlichtingendoeleinden zeer gericht is.

De wet brengt tevens aanzienlijke wijzigingen aan in de procedures voor de FISA-rechtbank, die zowel de transparantie verhogen als aanvullende waarborgen verstrekken dat de privacy wordt beschermd. Zoals hiervoor is opgemerkt, werd toestemming gegeven voor de oprichting van een permanent panel van geaccrediteerde advocaten met ervaring op het gebied van privacy en burgerlijke vrijheden, het verzamelen van inlichtingen, communicatietechnologie of andere relevante gebieden, die kunnen worden benoemd om voor de rechtbank te verschijnen als *amicus curiae* in gevallen waarin sprake is van omvangrijke of nieuwe rechtsinterpretaties. Deze advocaten hebben de bevoegdheid om juridische argumenten naar voren te brengen die de bescherming van de individuele privacy en burgerlijke vrijheden bevorderen, en hebben toegang tot alle informatie, waaronder vertrouwelijke informatie, die de rechtbank nodig acht voor het uitoefenen van hun taken ([8]).

De wet bouwt ook voort op de ongekende transparantie van de Amerikaanse overheid op het gebied van inlichtingenactiviteiten door de DNI, na raadpleging van de Attorney General, te verplichten elk besluit, bevel of advies dat is verstrekt door de FISA-rechtbank of het Foreign Intelligence Surveillance Court of Review openbaar te maken of een openbare samenvatting ervan te publiceren waarin een ingrijpende uitleg of interpretatie van een wetsbepaling is opgenomen.

([1]) Zie 50 U.S.C. § 1881f.
([2]) Zie id. § 1881a(l)(1).
([3]) Zie id. § 1881a(l)(3). Enkele van deze verslagen zijn vertrouwelijk.
([4]) Mem. Opinion en Order, punt 26 (FISC 2014), beschikbaar op http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf
([5]) Zie de USA FREEDOM Act van 2015, Pub. L. No. 114-23, § 401, 129 Stat. 268.
([6]) Zie id. §§ 103, 201, 501. National Security Letters worden toegestaan in meerdere federale wetten en stellen de FBI in staat om informatie te verkrijgen die is opgenomen in kredietverslagen, financiële gegevens en elektronische abonnements- en transactiegegevens van bepaalde soorten bedrijven, uitsluitend ter bescherming tegen internationaal terrorisme of clandestiene inlichtingenactiviteiten. Zie 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; 18 U.S.C. § 2709. National Security Letters worden voornamelijk gebruikt door de FBI voor het verzamelen van cruciale informatie zonder inhoud in de vroege stadia van onderzoeken in het kader van contra-terrorisme en contra-inlichtingen, zoals de identiteit van een abonnee van een account die mogelijk heeft gecommuniceerd met vertegenwoordigers van een terroristische groepering, zoals IS. Ontvangers van een National Security Letter kunnen deze aanvechten in de rechtbank. Zie 18 U.S.C. § 3511.
([7]) Zie id.
([8]) Zie id. § 401.

Bovendien voorziet de wet in uitgebreide openbaarmakingen over verzoeken om verzameling in het kader van de FISA of National Security Letters. De Verenigde Staten moeten elk jaar aan het Congres en aan het publiek het aantal FISA-bevelen en certificeringen dat is aangevraagd en verleend, bekendmaken; schattingen van het aantal Amerikanen en niet-Amerikanen die het voorwerp zijn geweest van surveillance of waarop surveillance betrekking heeft gehad; en het aantal benoemingen van *amici curiae*, in aanvulling op andere soorten informatie ([1]). De wet bevat tevens verplichtingen over aanvullende openbare verslaglegging door de overheid over de hoeveelheid verzoeken in National Security Letters over zowel Amerikanen als niet-Amerikanen ([2]).

Met betrekking tot de transparantie van bedrijven biedt de wet bedrijven een reeks opties om openbaar verslag te doen van het samengevoegde aantal FISA-bevelen en -richtlijnen van National Security Letters dat zij ontvangen van de overheid, evenals het aantal klantaccounts waarop deze bevelen gericht zijn ([3]). Verschillende bedrijven hebben reeds dergelijke informatie bekendgemaakt, waaruit het geringe aantal klanten blijkt waarvan om gegevens is verzocht.

Deze transparantieverslagen van bedrijven tonen aan dat de Amerikaanse inlichtingenverzoeken slechts betrekking hebben op een minuscule hoeveelheid gegevens. Het recente transparantieverslag van een grote onderneming laat bijvoorbeeld zien dat deze verzoeken in het kader van de nationale veiligheid ontving (overeenkomstig FISA of National Security Letters) die betrekking hadden op minder dan 20 000 van zijn accounts op een moment waarop de onderneming minstens 400 miljoen abonnees had. Met andere woorden: alle door deze onderneming gerapporteerde Amerikaanse verzoeken in het kader van de nationale veiligheid hadden betrekking op minder dan 0,005 % van zijn abonnees. Zelfs als al deze verzoeken betrekking hadden gehad op Safe Harbor-gegevens, wat uiteraard niet het geval is, is duidelijk dat deze verzoeken gericht zijn en een passende omvang hebben en niet bulksgewijs noch ongedifferentieerd plaatsvinden.

Tot slot heeft de wetgeving waarin National Security Letters worden toegestaan, de omstandigheden waaronder een ontvanger van een dergelijke brief kan worden verboden deze openbaar te maken, weliswaar reeds beperkt, maar deze wet voorziet er verder in dat dergelijke geheimhoudingsvereisten periodiek moeten worden herzien en dat ontvangers van een National Security Letter worden geïnformeerd wanneer de feiten een geheimhoudinsgvereiste niet langer ondersteunen; en heeft de procedures gecodificeerd waarmee ontvangers beroep kunnen instellen tegen geheimhoudingsvereisten ([4]).

Kortom, de belangrijke wijzigingen die de USA FREEDOM Act heeft aangebracht in de bevoegdheden van Amerikaanse inlichtingendiensten zijn een duidelijk bewijs van de uitgebreide inspanningen die de Verenigde Staten hebben ondernomen om de bescherming van persoonsgegevens, privacy, burgerlijke vrijheden en transparantie bij alle Amerikaanse inlichtingenpraktijken op de voorgrond te plaatsen.

IV. TRANSPARANTIE

In aanvulling op de transparantie die wordt voorgeschreven in de USA FREEDOM Act, verstrekken de Amerikaanse inlichtingendiensten het publiek nog veel meer informatie, zodat een sterk voorbeeld wordt gegeven ten aanzien van de transparantie in het kader van zijn inlichtingenactiviteiten. De inlichtingendiensten hebben veel van hun beleidsmaatregelen, procedures, besluiten van het Foreign Intelligence Surveillance Court en andere openbaar gemaakte inhoud gepubliceerd, zodat een uitzonderlijk hoge mate van transparantie is bereikt. Daarnaast hebben de inlichtingendiensten aanzienlijk meer statistieken bekendgemaakt over het gebruik door de overheid van de verzamelingsbevoegdheden in het kader van de nationale veiligheid. Op 22 april 2015 publiceerden de inlichtingendiensten hun tweede jaarverslag met statistieken over hoe vaak de overheid deze belangrijke bevoegdheden gebruikt. Het ODNI heeft op zijn website en op *IC On the Record* ook een reeks concrete transparantiebeginselen ([5]) en een uitvoeringsplan gepubliceerd dat de beginselen vertaalt naar concrete, meetbare initiatieven ([6]). In oktober 2015 gelastte de DNI dat elke inlichtingendienst een functionaris voor de transparantie van inlichtingen moest benomen om transparantie te bevorderen en leiding te geven aan transparantie-initiatieven ([7]). De transparantiefunctionaris werkt nauw samen met de functionaris voor privacy en burgerlijke vrijheden van elke inlichtingendienst om te verzekeren dat transparantie, privacy en burgerlijke vrijheden topprioriteiten blijven.

([1]) Zie id. § 602.
([2]) Zie id.
([3]) Zie id. § 603.
([4]) Zie id. §§ 502(f)-503.
([5]) Beschikbaar op http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles
([6]) Beschikbaar op http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf
([7]) Zie id.

Als voorbeeld van deze inspanningen heeft de verantwoordelijke functionaris voor privacy en burgerlijke vrijheden van de NSA de afgelopen jaren meerdere niet-vertrouwelijke verslagen vrijgegeven, waaronder verslagen over activiteiten op grond van sectie 702, uitvoeringsbevel 12333 en de USA FREEDOM Act ([1]). Daarnaast werken de inlichtingendiensten nauw samen met het PCLOB, het Congres en de Amerikaanse privacybelangenvereniging om waar mogelijk nog meer transparantie te bieden in verband met de Amerikaanse inlichtingenactiviteiten en in overeenstemming met de bescherming van gevoelige informatiebronnen en -methoden. Als geheel genomen zijn de Amerikaanse inlichtingenactiviteiten net zo transparant als of transparanter dan die van elk ander land in de wereld en zijn ze zo transparant als mogelijk, rekening houdend met de behoefte om gevoelige bronnen en methoden te beschermen.

De uitgebreide transparantie van de Amerikaanse inlichtingenactiviteiten samengevat:

— de inlichtingendiensten hebben duizenden pagina's aan rechtbankadviezen en procedures van instanties vrijgegeven en online geplaatst waarin de specifieke procedures en vereisten van onze inlichtingenactiviteiten worden beschreven. We hebben tevens verslagen vrijgegeven over de naleving door inlichtingendiensten van de toepasselijke beperkingen.

— senior medewerkers van inlichtingendiensten spreken vaak in het openbaar over de rollen en activiteiten van hun organisaties, waaronder beschrijvingen van nalevingsregelingen en waarborgen die van toepassing zijn op hun werkzaamheden.

— de inlichtingendiensten hebben meerdere aanvullende documenten vrijgegeven over de inlichtingenactiviteiten op grond van de Freedom of Information Act.

— de president heeft PPD-28 uitgevaardigd, waarin in het openbaar aanvullende beperkingen uiteen werden gezet over onze inlichtingenactiviteiten en het ODNI heeft twee openbare verslagen opgesteld over de tenuitvoerlegging van deze beperkingen.

— de inlichtingendiensten zijn nu wettelijk verplicht om belangrijke juridische adviezen die zijn verstrekt door de FISA-rechtbank of samenvattingen van deze adviezen, vrij te geven.

— de overheid is verplicht om jaarlijks verslag te doen van de mate waarin gebruik wordt gemaakt van bepaalde bevoegdheden op het gebied van de nationale veiligheid en bedrijven mogen dat ook doen.

— het PCLOB heeft verschillende gedetailleerde openbare verslagen opgesteld over inlichtingenactiviteiten en blijft dat ook doen.

— de inlichtingendiensten verstrekken uitgebreide vertrouwelijke informatie aan toezichtscommissies van het Congres.

— de DNI heeft transparantiebeginselen opgesteld die van toepassing zijn op de activiteiten van de inlichtingendiensten.

Deze uitgebreide transparantie wordt voortgezet. Eventuele informatie die openbaar wordt gemaakt, wordt uiteraard beschikbaar gemaakt voor zowel het ministerie van Handel als de Europese Commissie. De jaarlijkse herziening tussen het ministerie van Handel en de Europese Commissie over het privacyschild biedt mogelijkheden voor de Europese Commissie om eventuele vragen te stellen die zijn ontstaan naar aanleiding van nieuwe vrijgegeven informatie, evenals eventuele andere zaken die betrekking hebben op het privacyschild en de werking daarvan, en we begrijpen dat het ministerie, naar eigen goeddunken, vertegenwoordigers van andere instanties, waaronder de inlichtingendiensten, kan uitnodigen om deel te nemen aan deze herziening. Dit is uiteraard in aanvulling op het mechanisme van PPD-28 waarmee de lidstaten van de EU surveillancegerelateerde bekommernissen kenbaar kunnen maken aan een aangewezen functionaris van het ministerie van Buitenlandse Zaken.

V. RECHTSMIDDELEN

De Amerikaanse wetgeving voorziet in een aantal mogelijke rechtsmiddelen voor betrokkenen die het voorwerp zijn geweest van onrechtmatige elektronische surveillance ten behoeve van de nationale veiligheid. Op grond van de FISA is het recht op rechtsmiddelen in de Amerikaanse rechtbank niet beperkt tot Amerikanen. Een betrokkene die kan a

([1]) Beschikbaar op https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf

antonen dat hij belang heeft bij het aanhangig maken van een procedure, beschikt over de rechtsmiddelen om onrechtmatige elektronische surveillance in het kader van de FISA voor de rechter te laten komen. In de FISA is het personen die het voorwerp zijn geweest van onrechtmatige elektronische surveillance, bijvoorbeeld toegestaan Amerikaanse overheidsfunctionarissen in hun persoonlijke hoedanigheid aan te klagen voor geldelijke vergoedingen, waaronder schadeloosstelling en advocaatkosten. Zie 50 U.S.C. § 1810. Betrokkenen die kunnen aantonen dat zij belang hebben bij het aanhangig maken van een procedure, beschikken ook over civiele rechtsmiddelen voor schadevergoeding, waaronder proceskosten, tegen de Verenigde Staten wanneer informatie over hen die is verkregen door middel van elektronische surveillance in het kader van de FISA, onrechtmatig en bewust is gebruikt of openbaar gemaakt. Zie 18 U.S.C. § 2712. Indien de overheid voornemens is informatie te gebruiken of bekend te maken die is verkregen of is afgeleid uit elektronische surveillance van een benadeelde persoon in het kader van de FISA tegen die betrokkene tijdens juridische of administratieve procedures in de Verenigde Staten, dan moet de overheid vooraf deze intentie kenbaar maken aan de rechtbank en aan de betrokkene, die vervolgens de rechtmatigheid van de surveillance kan aanvechten en kan verzoeken om de informatie buiten beschouwing te laten. Zie 50 U.S.C. § 1806. Tot slot voorziet de FISA in strafrechtelijke sancties voor personen die bewust betrokken zijn bij onrechtmatige elektronische surveillance uit naam van de wet of die bewust informatie gebruiken of openbaar maken die is verkregen door middel van onrechtmatige surveillance. Zie 50 U.S.C. § 1809.

EU-burgers hebben andere mogelijkheden voor het aanwenden van rechtsmiddelen tegen Amerikaanse overheidsmedewerkers voor onrechtmatig gebruik door de overheid van of toegang tot gegevens, waaronder overheidsfunctionarissen die de wet schenden tijdens de onrechtmatige toegang tot of het gebruik van informatie voor vermeende doeleinden in het kader van de nationale veiligheid. De Computer Fraud en Abuse Act verbiedt de opzettelijke onbevoegde toegang (of het overschrijden van de bevoegde toegang) voor het verkrijgen van informatie van een financiële instelling, een computersysteem van de Amerikaanse overheid of een computer waartoe toegang wordt verkregen via internet, evenals dreigementen om beschermde computers te beschadigen in het kader van afpersing of fraude. Zie 18 U.S.C. § 1030. Iedereen, ongeacht nationaliteit, die schade of verlies lijdt als gevolg van een schending van deze wet kan de overtreder aanklagen (zo ook een overheidsfunctionaris) voor schadevergoeding en voorlopige of billijke genoegdoening op grond van sectie 1030(g), ongeacht of er strafrechtelijke vervolging is ingesteld, mits het gedrag minstens een van de in de wetgeving opgenomen omstandigheden omvat. De Electronic Communications Privacy Act (ECPA) reguleert de toegang van de overheid tot opgeslagen elektronische communicatie en transactiegegevens en informatie over abonnees in bezit van externe communicatieverleners. Zie 18 U.S.C. §§ 2701-2712. De ECPA staat een benadeelde persoon toe overheidsfunctionarissen aan te klagen voor opzettelijke onrechtmatige toegang tot opgeslagen gegevens. De ECPA is van toepassing op iedereen, ongeacht het staatsburgerschap en benadeelde personen kunnen schadevergoeding en advocaatkosten toegewezen krijgen. De Right to Financial Privacy Act (RFPA) beperkt de toegang van de Amerikaanse overheid tot gegevens van banken en makelaars-dealers van individuele personen. Zie 12 U.S.C. §§ 3401-3422. Op grond van de RFPA kan een klant van een bank of een makelaar-dealer de Amerikaanse overheid aanklagen voor wettelijke, daadwerkelijke en strafrechtelijke schade voor het onrechtmatig verkrijgen van toepassing tot de klantgegevens, en een oordeel dat deze onrechtmatige toegang opzettelijk was, leidt automatisch tot een onderzoek van mogelijke disciplinaire acties tegen de desbetreffende overheidsmedewerkers. Zie 12 U.S.C. § 3417.

Tot slot biedt de Freedom of Information Act (FOIA) middelen voor iedereen om toegang te vragen tot bestaande gegevens van federale instanties over elk voorwerp, behalve enkele uitzonderingscategorieën. Zie 5 U.S.C. § 552(b). Deze uitzonderingen zijn onder meer de toegang tot vertrouwelijke informatie over de nationale veiligheid, persoonlijke gegevens van derden en informatie over onderzoeken in het kader van rechtshandhaving en zijn vergelijkbaar met de beperkingen die door landen worden opgelegd in hun eigen wetgeving betreffende de toegang tot informatie. Deze beperkingen zijn gelijkelijk van toepassing op Amerikanen en niet-Amerikanen. In geschillen met betrekking tot de vrijgave van gegevens waarom is verzocht in het kader van de Freedom of Information Act, kan beroep worden ingesteld bij de administratieve rechtbank en vervolgens bij de federale rechter. De rechtbank moet opnieuw beoordelen of de gegevens terecht niet zijn vrijgegeven, 5 U.S.C. § 552(a)(4)(B), en kan de overheid dwingen toegang tot de gegevens te verlenen. De rechtbank heeft in sommige gevallen geoordeeld dat informatie die door de regering onterecht als vertrouwelijk werd aangemerkt, niet mocht worden achtergehouden ([1]). Hoewel er geen geldelijke compensatie beschikbaar is, kan de rechtbank wel de advocaatkosten toekennen.

VI. CONCLUSIE

De Verenigde Staten erkennen dat onze activiteiten in het kader van inlichtingen uit berichtenverkeer en andere inlichtingenactiviteiten er rekening mee moeten houden dat eenieder respectvol en waardig moet worden behandeld, ongeacht zijn nationaliteit of verblijfplaats, en dat iedereen rechtmatige privacybelangen heeft bij de hantering van persoonsgegevens. De Verenigde Staten maken uitsluitend gebruik van inlichtingen uit berichtenverkeer ter bevordering van de nationale veiligheid en belangen in het kader van buitenlands beleid en ter bescherming van zijn burgers en de burgers van zijn bondgenoten en partners tegen onrecht. De inlichtingendiensten zijn kortom niet betrokken bij de willekeurige surveillance van wie dan ook, waaronder gewone Europese burgers. De verzameling van inlichtingen uit berichtenverkeer vindt uitsluitend plaats wanneer dat naar behoren is toegestaan en op een wijze die strikt voldoet aan deze beperkingen; uitsluitend na beoordeling van de beschikbaarheid van alternatieve bronnen, waaronder diplomatieke en openbare

([1]) Zie bv. *New York Times v. Department of Justice*, 756 F.3d 100 (2d Cir. 2014); *American Civil Liberties Union v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

bronnen; en op een wijze waarop passende en haalbare alternatieven voorrang krijgen. En indien mogelijk vindt het verzamelen van inlichtingen uit berichtenverkeer uitsluitend plaats door deze te richten op specifieke doelwitten en onderwerpen van buitenlandse inlichtingen door middel van het gebruik van discriminanten.

Het Amerikaanse beleid in dit verband werd bevestigd in PPD-28. Binnen dit kader hebben de Amerikaanse inlichtingendiensten niet de wettelijke bevoegdheid, de middelen, de technische mogelijkheden of de wens om alle communicatie ter wereld te onderscheppen. Deze diensten lezen niet de e-mails van alle personen in de Verenigde Staten of wereldwijd. In overeenstemming met PPD-28 hebben de Verenigde Staten solide bescherming ingevoerd voor de persoonsgegevens van niet-Amerikanen die worden verzameld door middel van activiteiten in het kader van inlichtingen uit berichtenverkeer. Dit omvat, voor zover maximaal mogelijk en in overeenstemming met de nationale veiligheid, beleidsmaatregelen en procedures om de opslag en verspreiding van persoonsgegevens met betrekking tot niet-Amerikanen te minimaliseren, in vergelijking met de bescherming die wordt genoten door Amerikanen. Bovendien is, zoals hiervoor is besproken, de uitgebreide toezichtsregeling van de gerichte bevoegdheid in sectie 702 van de FISA ongekend. Tot slot verbeteren de omvangrijke wijzigingen in de Amerikaanse wetgeving ten aanzien van de inlichtingendiensten, zoals vastgesteld in de USA FREEDOM Act en de door het ODNI geleide initiatieven ter bevordering van de transparantie binnen de inlichtingendiensten, de privacy en burgerlijke vrijheden van eenieder aanzienlijk, ongeacht de nationaliteit van de betrokkene.

Met vriendelijke groet,

Robert S. Litt

21 juni 2016

Dhr. Justin S. Antonipillai
Counselor
Amerikaans ministerie van Handel
1401 Constitution Avenue, N.W.
Washington, DC 20230

Dhr. Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Avenue, N.W.
Washington, DC 20230

Geachte heren Antonipillai en Dean:

Ik schrijf u met nadere informatie over de wijze waarop de Verenigde Staten bulksgewijs inlichtingen uit berichtenverkeer verzamelen. Zoals toegelicht in voetnoot 5 van Presidential Policy Directive 28 (presidentiële richtlijn 28, hierna „PPD-28" genoemd), wordt met „bulksgewijze" verzameling bedoeld: het verkrijgen van een relatief groot volume informatie of gegevens uit berichtenverkeer onder omstandigheden waarin de inlichtingendiensten geen gebruik kunnen maken van een identificator die verband houdt met een specifiek doelwit (zoals het e-mailadres of telefoonnummer van het doelwit) waarop de verzameling wordt gericht. Dit wil echter niet zeggen dat het om „grootschalige" of „ongedifferentieerde" verzameling gaat. PPD-28 schrijft immers ook voor dat activiteiten op het gebied van inlichtingen uit berichtenverkeer zo gericht mogelijk moeten zijn. Ter bevordering van deze opdracht nemen de inlichtingendiensten maatregelen om ervoor te zorgen dat, zelf wanneer we geen specifieke identificatoren kunnen gebruiken om de verzameling op af te stemmen, de te verzamelen gegevens waarschijnlijk buitenlandse inlichtingen zullen bevatten die voldoen aan de vereisten van de Amerikaanse beleidsmakers op grond van de in mijn vorige brief uiteengezette procedure, en de hoeveelheid verzamelde niet-pertinente informatie wordt beperkt.

Aan de inlichtingendiensten kan bijvoorbeeld worden gevraagd om inlichtingen uit berichtenverkeer te verkrijgen over de activiteiten van een terroristische groepering die in een regio van een land in het Midden-Oosten actief is en waarvan wordt aangenomen dat zij aanslagen voorbereidt tegen West-Europese landen, waarbij zij mogelijk geen weet hebben van de namen, telefoonnummers, e-mailadressen of andere specifieke identificatoren van personen die banden hebben met deze groepering. Wij zouden er kunnen voor kiezen om ons op die groepering te richten door communicatie naar en vanuit die regio te verzamelen voor verder onderzoek en analyse, om na te gaan welke communicatie op deze groepering betrekking heeft. Zodoende zouden de inlichtingendiensten ernaar streven de verzameling zo beperkt mogelijk te houden. Dit zou worden beschouwd als „bulksgewijs" verzamelen omdat het gebruik van discriminanten niet haalbaar is, maar het is noch „grootschalig", noch „ongedifferentieerd"; het is veeleer zo nauwkeurig gericht mogelijk.

Zelfs wanneer doelgerichte verzameling met gebruik van selectietermen niet mogelijk is, verzamelt de VS derhalve niet alle communicatie van alle communicatievoorzieningen ter wereld, maar past het filters en andere technische hulpmiddelen toe om de verzameling af te stemmen op de voorzieningen via welke waarschijnlijk communicatie plaatsvindt die waardevolle buitenlandse inlichtingen bevat. Op die manier treffen de activiteiten van de Verenigde Staten met betrekking tot inlichtingen uit berichtenverkeer slechts een fractie van het communicatieverkeer via het internet.

Zoals in mijn vorige brief vermeld, vormt „bulksgewijs" verzamelen bovendien een groter risico op verzamelen van niet-pertinente communicatie en daarom beperkt PPD-28 het gebruik dat de inlichtingendiensten kunnen maken van bulksgewijs verzamelde inlichtingen uit berichtenverkeer tot zes specifieke doeleinden. PPD-28 en het beleid van de instanties die dat PPD-28 uitvoeren, beperken ook de bewaring en de verspreiding van persoonsgegevens die via inlichtingen uit berichtenverkeer zijn verkregen, ongeacht of de informatie bulksgewijs werd verzameld dan wel via gerichte verzameling en ongeacht de nationaliteit van de betrokkene.

De „bulksgewijze" verzameling door de inlichtingendiensten is niet „grootschalig" of „ongedifferentieerd", maar houdt de toepassing in van methoden en instrumenten voor het filteren van gegevensverzameling, om deze te richten op materiaal dat voldoet aan de vereisten van de beleidsmakers in verband met buitenlandse inlichtingen en tegelijkertijd de verzameling van niet-pertinente informatie tot een minimum beperkt. Er gelden ook strikte regels ter bescherming van

de niet-pertinente informatie die mogelijk wordt verkregen. Het beleid en de procedures die in deze brief worden beschreven, zijn van toepassing op alle verzameling van inlichtingen uit berichtenverkeer, met inbegrip van de bulksgewijze verzameling van communicatie van en naar Europa, zonder dat wordt bevestigd of ontkend dat dergelijke verzameling plaatsvindt.

U hebt tevens om meer informatie verzocht over de Privacy and Civil Liberties Oversight Board (Raad van toezicht op de privacy en de burgerlijke vrijheden, hierna „PCLOB" genoemd) en Inspectors General, en hun bevoegdheden. De PCLOB is een onafhankelijke instantie binnen de uitvoerende macht. In de raad zijn beide partijen vertegenwoordigd en zetelen vijf leden, die door de president worden benoemd en door de Senaat worden bekrachtigd ([1]). Elk lid van de raad heeft een ambtstermijn van zes jaar. De leden en het personeel van de raad beschikken over de nodige veiligheidsmachtigingen om hun wettelijke taken en verantwoordelijkheden ten volle te kunnen uitvoeren ([2]).

De PCLOB heeft als taak te zorgen voor een evenwicht tussen de inspanningen van de federale overheid om terrorisme te voorkomen enerzijds en de noodzaak om de privacy en de burgerlijke vrijheden te beschermen anderzijds. De Raad heeft twee fundamentele verantwoordelijkheden: toezicht en advies. Hij stelt zijn eigen agenda vast en bepaalt welke activiteiten op het gebied van toezicht en advies hij wenst uit te voeren.

In zijn *toezichthoudende* rol evalueert en analyseert de PCLOB maatregelen van de uitvoerende macht om het land tegen terrorisme te beschermen en zorgt hij ervoor dat de behoefte aan dergelijke maatregelen wordt afgewogen tegen de noodzaak de privacy en burgerlijke vrijheden te beschermen ([3]). De meest recent uitgevoerde toezichtsbeoordeling had betrekking op surveillanceprogramma's die krachtens sectie 702 van de FISA worden verricht ([4]). Momenteel verricht hij een evaluatie van inlichtingenactiviteiten in het kader van Executive Order 12333 ([5]).

In zijn *adviserende* rol zorgt de PCLOB ervoor dat er terdege rekening wordt gehouden met kwesties op het gebied van vrijheden bij de ontwikkeling en uitvoering van wet- en regelgeving, en van beleidsmaatregelen om het land tegen terrorisme te beschermen ([6]).

Om zijn taken te vervullen is de raad bij wet gemachtigd om toegang te krijgen tot alle relevante gegevens, verslagen, audits, evaluaties, documenten, aanbevelingen en eventuele andere relevante informatie van instanties, waaronder ook gerubriceerde informatie overeenkomstig de wet ([7]). Voorts kan de raad een gesprek hebben met of verklaringen of openbare getuigenissen afnemen van een ambtenaar of personeelslid van de uitvoerende macht ([8]). Bovendien kan de raad de Attorney General schriftelijk verzoeken om namens de raad dwangbevelen uit te vaardigen waarbij partijen buiten de uitvoerende macht gedwongen worden om relevante informatie te verstrekken ([9]).

Ten slotte gelden voor de PCLOB wettelijke voorschriften inzake openbare transparantie. Dit houdt onder meer in dat het publiek zoveel mogelijk op de hoogte wordt gehouden van zijn activiteiten via openbare hoorzittingen en toegang krijgt tot zijn verslagen, voor zover dat in overeenstemming is met de bescherming van gerubriceerde gegevens ([10]). Voorts moet de PCLOB verslag uitbrengen wanneer een dienst van de uitvoerende macht weigert zijn advies te volgen.

Inspectors General (inspecteurs-generaal, hierna „IG's" genoemd) in de Intelligence Community (inlichtingendiensten, hierna „IC" genoemd) voeren audits, inspecties, en evaluaties van de programma's en activiteiten in de IC uit om systeemrisico's, kwetsbaarheden en tekortkomingen vast te stellen en aan te pakken. Voorts onderzoeken IG's klachten of

([1]) 42 U.S.C. 2000ee(a), (h).
([2]) 42 U.S.C. 2000ee(k).
([3]) 42 U.S.C. 2000ee(d)(2).
([4]) Zie in het algemeen https://www.pclob.gov/library.html#oversightreports
([5]) Zie in het algemeen https://www.pclob.gov/events/2015/may13.html
([6]) 42 U.S.C. 2000ee(d)(1); zie ook PCLOB Advisory Function Policy and Procedure, Policy 2015-004, beschikbaar op https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf
([7]) 42 U.S.C. 2000ee(g)(1)(A).
([8]) 42 U.S.C. 2000ee(g)(1)(B).
([9]) 42 U.S.C. 2000ee(g)(1)(D).
([10]) 42 U.S.C. 2000eee(f).

informatie van vermeende schendingen van wet- of regelgeving of wanbeheer, grove verspilling van middelen, misbruik van gezag of een aanzienlijk of specifiek gevaar voor de volksgezondheid en de openbare veiligheid in IC-programma's en -activiteiten. De onafhankelijkheid van IG's is een essentieel onderdeel van de objectiviteit en integriteit van elk verslag, elke vaststelling en elke aanbeveling van een IG. Een aantal van de meest essentiële elementen voor het garanderen van de onafhankelijkheid van IG's, heeft betrekking op hun benoeming en ontslag, afzonderlijke operationele, begrotings- en personele autoriteiten, en dubbele rapportageverplichtingen aan de instellingshoofden van de uitvoerende macht en het congres.

Het Congres heeft een onafhankelijke IG-dienst opgericht in elke instelling van de uitvoerende macht, met inbegrip van elk onderdeel van de IC ([1]). Na de aanneming van de Intelligence Authorization Act for Fiscal Year 2015 worden bijna alle IG's die toezicht houden op een onderdeel van de IC, benoemd door de president en bevestigd door de Senaat. Dat is onder meer het geval bij het Department of Justice, het Central Intelligence Agency, het National Security Agency en de Intelligence Community ([2]). Deze IG's zijn voorts permanente en onpartijdige ambtenaren die alleen door de president kunnen worden afgezet. De Amerikaanse grondwet bepaalt weliswaar dat de president bevoegd is om IG's af te zetten, maar deze bevoegdheid werd slechts zelden uitgeoefend en vereist dat de president 30 dagen voor de afzetting van een IG het Congres een schriftelijke rechtvaardiging verstrekt ([3]). Deze procedure voor de benoeming van een IG zorgt ervoor dat er geen sprake is van ongeoorloofde inmenging van functionarissen van de uitvoerende macht in de selectie, benoeming of afzetting van een IG.

In de tweede plaats beschikken IG's over aanzienlijke wettelijke bevoegdheden om audits, onderzoeken en evaluaties van programma's en operaties van de uitvoerende macht uit te voeren. Naast de wettelijk voorgeschreven toezichtsonderzoeken en evaluaties, beschikken IG's over een ruime beoordelingsvrijheid om hun toezichtsbevoegdheid uit te oefenen om de programma's en activiteiten van hun keuze te evalueren ([4]). De wet bepaalt dat de IG's bij de uitoefening van deze bevoegdheid over de onafhankelijke middelen moeten beschikken om hun taken uit te voeren, met inbegrip van de bevoegdheid om hun eigen personeel in dienst te nemen en hun begrotingsverzoeken aan het Congres afzonderlijk te documenteren ([5]). De wet garandeert dat IG's toegang hebben tot de informatie die zij nodig hebben voor de uitvoering van hun taken. Daarbij gaat het onder meer om de bevoegdheid om directe toegang te krijgen tot alle gegevens en informatie van de instellingen over hun programma's en activiteiten, ongeacht de classificatie ervan; de bevoegdheid om informatie en documenten op te vorderen; en de bevoegdheid om een eed af te nemen ([6]). In een beperkt aantal gevallen mag het hoofd van een instelling van de uitvoerende macht de activiteit van een IG verbieden wanneer bijvoorbeeld een audit of onderzoek van een IG de nationale veiligheidsbelangen van de Verenigde Staten aanmerkelijk zou schaden. Ook de uitoefening van deze bevoegdheid is zeer ongebruikelijk en vereist dat het hoofd van de instelling binnen 30 dagen het Congres in kennis stelt van de redenen waarom deze bevoegdheid wordt uitgeoefend ([7]). De DNI heeft nooit gebruikgemaakt van deze beperking van de bevoegdheid van IG-activiteiten.

Ten derde zijn de IG's er verantwoordelijk voor zowel de hoofden van de instellingen van de uitvoerende macht als het Congres ten volle en voortdurend via verslagen in te lichten over fraude en andere ernstige problemen, misbruiken en tekortkomingen in verband met de programma's en activiteiten van de uitvoerende macht ([8]). De dubbele rapportage versterkt de onafhankelijkheid van de IG's door te zorgen voor transparantie in de toezichtprocedure en biedt de hoofden van de instellingen de kans om de aanbevelingen van de IG uit te voeren voordat het Congres wetgevende maatregelen kan nemen. De IG's zijn bijvoorbeeld wettelijk verplicht om halfjaarlijkse verslagen op te stellen waarin dergelijke problemen samen met tot dusver genomen maatregelen worden beschreven ([9]). De instellingen van de uitvoerende macht moeten de vaststellingen en aanbevelingen van de IG's ernstig nemen en de IG's zijn dikwijls in staat

([1]) Secties 2 en 4 van de Inspector General Act van 1978, zoals gewijzigd (hierna: IG Act); Sectie 103(b) en (e), van de National Security Act van 1947, zoals gewijzigd (hierna „at'l Sec. Act\". Sectie 17(a), van de Central Intelligence Act (hierna „CIA Act").

([2]) Zie Pub. L. No. 113-293, 128 Stat. 3990, (19 dec. 2014). Alleen de IG's voor het Defense Intelligence Agency en het National Geospatial-Intelligence Agency worden niet door de president benoemd; de IG DOD en de IG IC hebben gedeelde bevoegdheid over deze instanties.

([3]) Sectie 3 van de IG Act van 1978, zoals gewijzigd; sectie 103H(c) van de Nat'l Sec. Act; en sectie 17(b) van de CIA Act.

([4]) Zie Secties 4(a) en 6(a)(2) van de IG Act 1947; Sectie 103H(e) en (g)(2)(A) van de Nat'l Sec. Act; Sectie 17(a) en (c) van de CIA Act.

([5]) Secties 3(d), 6(a)(7) en 6(f) van de IG Act; Secties 103H(d), (i), (j) en (m) van de Nat'l Sec. Act; Secties 17(e)(7) en (f) van de CIA Act.

([6]) Sectie 6(a)(1), (3), (4), (5), en (6) van de IG Act; Secties 103H(g)(2) van de Nat'l Sec. Act; Sectie 17(e)(1), (2), (4), en (5) van de CIA Act.

([7]) Zie bv. secties 8(b) en 8E(a) van de IG Act; Sectie 103H(f) van de Nat'l Sec. Act; Sectie 17(b) van de CIA Act.

([8]) Sectie 4(a)(5) van de IG Act; Sectie 103H(a)(b)(3) en (4) van de Nat'l Sec. Act; Sectie 17(a)(2) en (4) van de CIA Act.

([9]) Sectie 2(3), 4(a), en 5 van de IG Act; Sectie 103H(k) van de Nat'l Sec. Act; Sectie 17(d) van de CIA Act. De inspecteur-generaal van het ministerie van Justitie maakt zijn publiek vrijgegeven verslagen op het internet beschikbaar op http://oig.justice.gov/reports/all.htm. Zo ook maakt de inspecteur-generaal voor de inlichtingendiensten zijn halfjaarlijkse verslagen voor het publiek beschikbaar op https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig

om de aanvaarding en tenuitvoerlegging van IG-aanbevelingen door de instellingen op te nemen in deze en andere verslagen die aan het Congres, en in sommige gevallen aan het publiek, worden verstrekt ([1]). Naast deze structuur van dubbele rapportage, zijn de IG's er ook verantwoordelijk voor klokkenluiders in de uitvoerende macht tot bij de passende parlementaire comités voor toezicht te leiden waar zij vermseende fraude, verspilling en misbruik in programma's en activiteiten van de uitvoerende macht kunnen melden. De identiteit van personen die zich aanmelden, wordt tegen openbaarmaking aan de uitvoerende macht beschermd, waardoor de klokkenluiders worden beschermd tegen mogelijke verboden personeelsmaatregelen of maatregelen inzake veiligheidsmachtiging als represaille voor de melding aan de IG ([2]). Aangezien klokkenluiders dikwijls de bron vormen van IG-onderzoek, vergroot het feit dat zij hun bekommernissen aan het Congres kunnen melden zonder beïnvloeding door de uitvoerende macht, de doeltreffendheid van het IG-toezicht. Door deze onafhankelijkheid kunnen IG's de zuinigheid, efficiëntie en verantwoordingsplicht van instellingen van de uitvoerende macht bevorderen met objectiviteit en integriteit.

Ten slotte heeft het Congres de Council of Inspectors General on Integrity and Efficiency (de raad van inspecteurs voor integriteit en efficiëntie) opgericht. Deze raad ontwikkelt onder meer IG-normen voor audits, onderzoeken en evaluaties, bevordert opleiding en is bevoegd om beschuldigingen van wangedrag door IG's te beoordelen. Zo houdt deze raad een kritische blik op de IG's, die zelf belast zijn met het toezicht op alle anderen ([3]).

Ik hoop u met deze informatie van dienst te zijn geweest.

Met vriendelijke groet,
Robert S. Litt
General Counsel

([1]) Sectie 2(3), 4(a), en 5 van de IG Act; Sectie 103H(k) van de Nat'l Sec. Act; Sectie 17(d) van de CIA Act. De inspecteur-generaal van het ministerie van Justitie maakt zijn publiek vrijgegeven verslagen op het internet beschikbaar op http://oig.justice.gov/reports/all.htm. Zo ook maakt de inspecteur-generaal voor de inlichtingendiensten zijn halfjaarlijkse verslagen voor het publiek beschikbaar op https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig

([2]) Sectie 7 van de IG Act; Sectie 103H(g)(3) van de Nat'l Sec. Act; Sectie 17(e)(3) van de CIA Act.

([3]) Sectie 11 van de IG Act.

BIJLAGE VII

Brief van Deputy Assistant Attorney General en Counselor for International Affairs Bruce Swartz, Amerikaans ministerie van Justitie

19 februari 2016

Dhr. Justin S. Antonipillai
Counselor
Amerikaans ministerie van Handel
1401 Constitution Ave., NW
Washington, DC 20230

Dhr. Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Geachte heren Antonipillai en Dean:

Deze brief bevat een kort overzicht van de primaire onderzoeksmiddelen die worden gebruikt om commerciële gegevens en andere opgeslagen gegevens van bedrijven in de Verenigde Staten te verkrijgen in het kader van strafrechtelijke vervolging of het openbaar belang (civiele en regelgevende doeleinden), waaronder de toegangsbeperkingen die zijn vastgesteld in deze bevoegdheden ([1]). Deze 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-privacyschildkader, ongeacht de nationaliteit 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.". 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) (*citing Camara v. Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). 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 v. United States*, 389 U.S. 347, 357 (1967). Als het vereiste van een huiszoekingsbevel niet van toepassing is, zijn activiteiten van de overheid 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.

Strafrechtelijke wetshandhavingsinstanties:

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

([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, zie 12 U. S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, en voor elektronische surveillance, huiszoekingsbevelen, bedrijfsgegevens en overige verzameling van communicatie op grond van de Foreign Intelligence Surveillance Act, Zie 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 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 waarborgen die zijn opgenomen in de grondwet van de staat en 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.

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. P. 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 te overleggen 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 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 realtime bel-, routing-, adres- 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 de telefoonbedrijven van internetleveranciers, 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 internetleveranciers. De SCA voorziet in hogere niveaus van privacywaarborgen, afhankelijk van de indringendheid van de verzameling. Voor het verkrijgen van informatie over abonnees, IP-adressen en bijbehorende tijdcodes, evenals van factuurinformatie moeten strafrechtelijke handhavingsinstanties een dwangbevel verkrijgen. Voor de meeste andere niet inhoudgerelateerde 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 strafrechtelijke wetshandhavingsinstanties over het algemeen een huiszoekingsbevel verkrijgen van een rechter op basis van gerede aanleiding om aan te nemen dat de desbetreffende account bewijs bevat van een misdrijf. De SCA voorziet tevens in civiele aansprakelijkheid en strafrechtelijke sancties.

Gerechtelijke bevelen voor surveillance op grond van federale wetgeving inzake afluisteren: Daarnaast kunnen wetshandhavingsinstanties mondelinge of elektronische communicatie in realtime onderscheppen ten behoeve van strafrechtelijk onderzoek op grond van federale wetgeving inzake afluisteren. Zie 18 U.S.C. §§ 2510-2522. 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 — Regel 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 „gerede aanleiding" dat er een misdrijf is gepleegd of zal worden gepleegd en dat zaken die verband houden met de 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. Zie U.S. Const. amend. IV (zoals hiervoor in detail besproken), Fed. R. Crim. P. 41. Degene tegen wie een huiszoekingsbevel gericht is, kan verzoeken het bevel nietig te verklaren als gevolg van een te brede formulering, of omdat het vexatoir of anderszins op onjuiste wijze is verkregen en benadeelden met procesbevoegdheid kunnen een motie indienen om bewijs dat bij een onrechtmatige huiszoeking is verkregen, buiten beschouwing te laten. Zie *Mapp v. Ohio*, 367 U.S. 643 (1961).

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 Federal Bureau of Investigation (FBI) Operations (september 2008) (hierna „AG FBI Guidelines" genoemd), beschikbaar op http://www.justice.gov/archive/opa/docs/guidelines.pdf, stellen beperkingen vast aan het gebruik van onderzoeksmiddelen om informatie te onderzoeken 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 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, 5. De FBI heeft deze richtsnoeren ten uitvoer gelegd door middel van de FBI Domestic Investigations and Operations Guide (DIOG), beschikbaar op https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20 (DIOG), een uitgebreid handboek met gedetailleerde beperkingen aan het gebruik van onderzoeksmiddelen en richtsnoeren om te verzekeren dat burgerlijke vrijheden en privacy in elk onderzoek worden beschermd. Aanvullende voorschriften en beleidsmaatregelen waarin beperkingen aan onderzoeksactiviteiten van federale aanklagers zijn vastgesteld, zijn opgenomen in het **United States Attorneys' Manual** (USAM), dat ook online beschikbaar is op http://www.justice.gov/usam/united-states-attorneys-manual.

Civiele en regelgevende instanties (openbaar belang)

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. P. 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. Zie 31 U.S.C. § 5318, 31 C.F.R. Part X. Andere bedrijven kunnen een beroep doen op de Fair Credit Reporting Act, zie 15 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. §§ 3401-3422. 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 van het vierde amendement. Zie *See v. 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 Attorney General 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.

Met vriendelijke groet,

Bruce C. Swartz

Deputy Assistant Attorney General and Counselor for International Affairs