EUROPESE
COMMISSIE

Brussel, 27.11.2013
COM(2013) 847 final

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

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

1. INLEIDING

Richtlijn 95/46/EG 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 (hierna "gegevensbeschermingsrichtlijn" genoemd) bevat de regels voor doorgifte van persoonsgegevens uit EU-lidstaten naar andere landen buiten de EU[1] voor zover die doorgifte binnen de werkingssfeer van dat instrument valt[2].

Op grond van de richtlijn kan de Commissie constateren dat een derde land, op grond van zijn nationale wetgeving of zijn internationale verbintenissen, een passend beschermingsniveau biedt met het oog op de bescherming van de rechten van personen, in welk geval de specifieke beperkingen inzake gegevensdoorgifte naar een dergelijk land niet van toepassing zouden zijn. Deze besluiten worden doorgaans "**besluiten inzake de gepastheid**" genoemd.

Op 26 juli 2000 heeft de Commissie Beschikking 2000/520/EG[3] aangenomen (hierna "**veiligehavenbeschikking**" genoemd), waarin werd erkend dat de veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de vaak gestelde vragen (hierna respectievelijk "beginselen" en "FAQs" genoemd), die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd, passende bescherming bieden in het kader van de doorgifte van persoonsgegevens uit de EU. De veiligehavenbeschikking werd aangenomen na een advies van de Groep artikel 29 en een advies van het Comité artikel 31, gegeven door een gekwalificeerde meerderheid van lidstaten. Overeenkomstig Besluit 1999/468 van de Raad werd de veiligehavenbeschikking eerst door het Europees Parlement onderzocht.

Dientengevolge staat de huidige veiligehavenbeschikking de vrije doorgifte[4] toe van persoonsgegevens uit de EU-lidstaten[5] naar ondernemingen in de VS die de beginselen hebben onderschreven, in omstandigheden waarin de doorgifte anders niet aan de EU-normen voor een passend niveau van gegevensbescherming zou voldoen, gelet op de substantiële verschillen tussen de privacyregelingen aan beide zijden van de Atlantische Oceaan.

De werking van de huidige veiligehavenregeling berust op verbintenissen en zelfcertificering van deelnemende ondernemingen. Deze regeling wordt vrijwillig onderschreven, maar de regels zijn bindend voor ondernemingen die de regeling hebben onderschreven. De grondbeginselen van die regeling zijn:

---

1 De artikelen 25 en 26 van de gegevensbeschermingsrichtlijn voorzien in het rechtskader voor doorgifte van persoonsgegevens uit de EU naar derde landen buiten de EER.

2 Aanvullende voorschriften zijn vastgesteld in artikel 13 van Kaderbesluit 2008/977/JBZ van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, voor zover deze doorgifte betrekking heeft op persoonsgegevens die door een lidstaat zijn verstrekt of beschikbaar gesteld aan een andere lidstaat, die vervolgens voornemens is deze gegevens aan een derde staat of internationale instelling door te geven met het oog op de preventie, het onderzoek, de opsporing en de vervolging ter zake van strafbare feiten en de tenuitvoerlegging van straffen.

3 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 ministerie van Handel van de Verenigde Staten zijn gepubliceerd (PB L 215 van 25.8.2000, blz. 7).

4 Het bovenstaande sluit niet uit dat op de gegevensverwerking andere vereisten van toepassing zijn krachtens nationale wetgeving tot uitvoering van de gegevensbeschermingsrichtlijn van de EU.

5 Hetzelfde geldt voor gegevensdoorgifte uit de drie staten die partij zijn bij de EER als gevolg van de uitbreiding van Richtlijn 95/46/EG tot de EER-overeenkomst, Besluit 38/1999 van 25 juni 1999, PB L 296 van 23.11.2000, blz. 41.

a) transparantie van het privacybeleid van de deelnemende ondernemingen,

b) opname van de veiligehavenbeginselen in het privacybeleid van die ondernemingen, en

c) handhaving, onder meer door de overheid.

Deze grondslagen van de veilige haven moeten worden herzien in de **nieuwe context** van:

a) de exponentiële groei van gegevensstromen, die vroeger accessoir waren, maar nu centraal staan in de snelle groei van de digitale economie en de zeer belangrijke ontwikkelingen in de verzameling, verwerking en gebruik van gegevens,

b) het cruciale belang van gegevensstromen, met name voor de trans-Atlantische economie,[6]

c) de snelle toename van het aantal ondernemingen in de VS die de veiligehavenregeling onderschrijven (sinds 2004 is dat verachtvoudigd, van 400 in 2004 tot 3 246 in 2013),

d) de recentelijk vrijgegeven informatie over Amerikaanse observatieprogramma's die nieuwe vragen doet rijzen over het beschermingsniveau dat de veiligehavenregeling geacht wordt te waarborgen.

Tegen deze achtergrond wordt in deze mededeling de balans opgemaakt van de werking van de veiligehavenregeling. Zij is **gebaseerd op gegevens** die door de Commissie zijn verzameld, de werkzaamheden van de EU-VS contactgroep privacy in 2009, een in 2008 door een onafhankelijke contractant uitgevoerde studie[7] en informatie die werd verkregen in de EU-VS ad hoc-werkgroep (hierna "werkgroep" genoemd), die werd opgericht na de onthullingen over Amerikaanse observatieprogramma's *(zie een parallel document)*. Deze mededeling is een vervolg op de twee **beoordelingsverslagen van de Commissie** in de opstartfase van de veiligehavenregeling, respectievelijk van 2002[8] en 2004[9].

2. STRUCTUUR EN WERKING VAN DE VEILIGEHAVENREGELING

2.1. Structuur van de veiligehavenregeling

Een onderneming uit de VS die aan de veilige haven wil deelnemen, moet: (a) in haar publiek toegankelijk privacybeleid vaststellen dat zij de beginselen onderschrijft en ook werkelijk naleeft, en (b) een zelfcertificering indienen, dat wil zeggen aan het ministerie van Handel van de VS verklaren dat zij overeenkomstig de beginselen handelt. De zelfcertificering moet jaarlijks opnieuw worden ingediend. De veiligehavenbeginselen, die zijn opgenomen in bijlage I bij de veiligehavenbeschikking, bevatten eisen met betrekking tot zowel de inhoudelijke bescherming van persoonsgegevens (beginselen inzake de integriteit,

---

6 Mochten de dienstenstromen en grensoverschrijdende gegevensstromen worden verstoord als gevolg van het stopzetten van *binding corporate rules* (gedragscodes voor de verwerking van persoonsgegevens binnen internationale concerns), modelcontractbepalingen en de veiligehavenregeling, dan zou volgens bepaalde studies het bbp van de EU kunnen dalen met 0,8 % tot 1,3 % en zou de uitvoer van diensten uit de EU naar de VS met 6,7 % dalen als gevolg van het verlies van concurrentievermogen. Zie: "*The Economic Importance of Getting Data Protection Right*", een studie van het European Centre for International Political Economy voor de US Chamber of Commerce, maart 2013.

7 Effectbeoordeling die in 2008 voor de Commissie is opgesteld door het *Centre de Recherche Informatique et Droit* ('CRID') van de universiteit van Namen.

8 Werkdocument van de diensten van de Commissie over de toepassing van Beschikking 520/2000/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 ministerie van Handel van de Verenigde Staten zijn gepubliceerd, SEC (2002) 196, 13.12.2002.

9 Werkdocument van de diensten van de Commissie over de tenuitvoerlegging van Beschikking 520/2000/EG van de Commissie 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 ministerie van Handel van de Verenigde Staten zijn gepubliceerd, SEC (2004) 1323, 20.10.2004.

beveiliging, keuze en verdere doorgifte van gegevens) als de procedurele rechten van de betrokkenen (beginselen inzake kennisgeving, toegang en handhaving).

Wat de handhaving van de veiligehavenregeling in de VS betreft, spelen twee belangrijke Amerikaanse instellingen een belangrijke rol: het ministerie van Handel en de Federal Trade Commission.

Het **ministerie van Handel** controleert elke nieuwe zelfcertificering voor de veilige havenregeling en elke jaarlijkse aanvraag voor een hernieuwde certificering die het van ondernemingen ontvangt, om ervoor te zorgen dat deze alle elementen bevatten die vereist zijn om aan de regeling deel te nemen[10]. Het ministerie werkt de lijst van ondernemingen bij die zelfcertificeringsbrieven hebben ingediend en publiceert de lijst en de brieven op zijn website. Bovendien houdt het toezicht op de werking van de veiligehavenregeling en verwijdert het ondernemingen die zich niet aan de beginselen houden, van de lijst.

De **Federal Trade Commission** treedt, binnen het kader van haar bevoegdheden op het gebied van consumentenbescherming, op tegen oneerlijke of misleidende praktijken overeenkomstig artikel 5 van de Free Trade Commission Act. De handhavingsmaatregelen van de Federal Trade Commission betreffen onder meer onderzoek naar valse verklaringen tot onderschrijving van de veiligehavenbeginselen en naar niet-naleving van die beginselen door de ondernemingen die aan de regeling deelnemen. In het specifieke geval van handhaving van de veiligehavenbeginselen tegen luchtvaartmaatschappijen, is de bevoegde instantie is het ministerie van Vervoer[11].

De huidige veiligehavenbeschikking maakt deel uit van het EU-recht dat door de autoriteiten van de lidstaten moet worden toegepast. Op grond van deze beschikking hebben de nationale **gegevensbeschermingsautoriteiten** van de EU het recht om in specifieke gevallen gegevensdoorgifte naar in het kader van de veilige haven gecertificeerde ondernemingen op te schorten[12]. De Commissie is geen geval bekend van opschorting door een nationale gegevensbeschermingsautoriteit sinds de invoering van de veiligehavenregeling in 2000. Onafhankelijk van de bevoegdheden waarover de nationale gegevensbeschermingsautoriteiten van de EU beschikken op grond van de veiligehavenbeschikking, zijn zij bevoegd om onder meer in het geval van internationale doorgifte, op te treden om ervoor te zorgen dat de algemene gegevensbeschermingsbeginselen uit de gegevensbeschermingsrichtlijn van 1995 worden nageleefd.

Zoals in de huidige veiligehavenbeschikking wordt herhaald, **staat het aan de Commissie** om – overeenkomstig de in Verordening 182/2011 bedoelde onderzoeksprocedure – te allen tijde de beschikking aan te passen of op te schorten, dan wel de werkingssfeer ervan te beperken in het licht van de bij de uitvoering ervan opgedane ervaringen. Dit geldt met name wanneer er sprake is van een systematische tekortkoming in de VS, bijvoorbeeld wanneer een orgaan dat verantwoordelijk is voor het waarborgen van de naleving van de veiligehavenbeginselen in de Verenigde Staten, niet daadwerkelijk zijn rol vervult, of wanneer het beschermingsniveau dat de veiligehavenbeginselen bieden, door de vereisten uit de wetgeving van de VS wordt

---

10 Indien de certificering of hercertificering van een onderneming niet aan de vereisten van de veiligehavenregeling voldoet, stelt het ministerie van Handel de onderneming in kennis van de te nemen stappen (bv. verduidelijkingen, wijzigingen in de beleidsbeschrijving) vóór de certificering kan worden afgerond.

11 Op grond van titel 49, artikel 41712 van de US Code.

12 Meer in het bijzonder kan in twee situaties de opschorting van doorgifte vereist zijn, nl. wanneer:
a) de overheidsinstantie in de VS heeft vastgesteld dat de onderneming de veiligehavenbeginselen schendt, of
b) het zeer waarschijnlijk is dat de veiligehavenbeginselen worden geschonden; er redelijkerwijs kan worden aangenomen dat het desbetreffende handhavingsmechanisme niet tijdig passende maatregelen neemt of zal nemen om het betrokken probleem op te lossen; zich een risico voordoet dat de betrokkenen ernstige schade wordt toegebracht wanneer verder gegevens worden doorgegeven; en de bevoegde autoriteiten in de lidstaat zich naar omstandigheden redelijke inspanningen hebben getroost om de onderneming van het probleem in kennis te stellen en de gelegenheid te geven te reageren.

achterhaald. Zoals elke andere beschikking van de Commissie, kan zij ook om andere redenen worden gewijzigd of zelfs ingetrokken.

2.2. De werking van de veiligehavenregeling

Onder de **3246**[13] **gecertificeerde ondernemingen** bevinden zich zowel kleine als grote ondernemingen[14]. De sectoren financiële diensten en telecommunicatie vallen weliswaar buiten de handhavingsbevoegdheden van de Federal Trade Commission en zijn derhalve uitgesloten van de veiligehavenregeling, maar toch zijn heel wat industriële en dienstensectoren vertegenwoordigd onder de gecertificeerde ondernemingen, waaronder bekende internetondernemingen en bedrijfstakken, variërend van informatie- en computerdiensten tot geneesmiddelen, reizen en toerisme, gezondheidszorg of kredietkaartdiensten[15]. Het gaat dan voornamelijk om Amerikaanse ondernemingen die diensten verlenen op de interne markt van de EU. Het gaat ook om dochterondernemingen van sommige ondernemingen uit de EU, zoals Nokia of Bayer. 51% zijn ondernemingen die gegevens van werknemers in Europa verwerken die zijn doorgegeven aan de VS in het kader van het personeelsbeheer[16].

Bij sommige gegevensbeschermingsautoriteiten in de EU is er **toenemende bezorgdheid** over de doorgifte van gegevens in het kader van de huidige veiligehavenregeling. Sommige gegevensbeschermingsautoriteiten van de lidstaten hebben kritiek op de zeer algemene formulering van de beginselen en de hoge afhankelijkheid van zelfcertificering en zelfregulering. Het bedrijfsleven heeft een soortgelijke bezorgdheid geuit met betrekking tot de verstoring van de mededinging als gevolg van een gebrek aan handhaving.

De huidige veiligehavenregeling is gebaseerd op de vrijwillige deelneming van ondernemingen, op zelfcertificering door deze deelnemende ondernemingen en op handhaving door overheidsinstanties van de uit de zelfcertificering voortvloeiende verbintenissen. In dit verband zouden een gebrek aan transparantie en eventuele tekortkomingen in de handhaving de grondvesten ondermijnen waarop de veiligehavenregeling is gebouwd.

Elke leemte in transparantie of handhaving in de VS leidt ertoe dat de verantwoordelijkheid komt te liggen bij de Europese gegevensbeschermingsautoriteiten en de ondernemingen die van de regeling gebruikmaken. Op 29 april 2010 hebben Duitse gegevensbeschermingsautoriteiten een besluit genomen op grond waarvan ondernemingen die aan de VS gegevens doorgeven, actief moeten nagaan of de ondernemingen in de VS die gegevens importeren, daadwerkelijk de veiligehavenbeginselen naleven en wordt aanbevolen dat ten minste de exporterende onderneming moet vaststellen of de veiligehavencertificering door de invoerder nog geldig is[17].

---

13 Op 26 september 2013 bedroeg het aantal veiligehavenorganisaties dat als "**actueel**" staat aangemerkt op de veiligehavenlijst **3246,** en als "**niet actueel**" **935.**

14 Veiligehavenorganisaties met 250 of minder werknemers: 60**%** (1925 van 3246). Veiligehavenorganisaties met 251 of meer werknemers: **40%** (1295 van 3246).

15 MasterCard bijvoorbeeld doet zaken met duizenden banken en de onderneming is een duidelijk voorbeeld van een geval waarin de veilige haven niet kan worden vervangen door andere rechtsinstrumenten voor de doorgifte van persoonsgegevens, zoals binding corporate rules of contractbepalingen.

16 Veiligehavenorganisaties die personeelsgegevens beheren in het kader van hun veiligehavencertificering (en er aldus mee hebben ingestemd samen te werken met en zich te schikken naar de gegevensbeschermingsautoriteiten van de EU): **51 %** (1671 van 3246).

17 Zie besluit van de Düsseldorfer Kreis van 28/29 april 2010 . Zie: Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile De Europese toezichthouder voor gegevensbescherming, Peter Hustinx, nam tijdens het onderzoek van de LIBE-commissie van het Europees Parlement op 7 oktober 2013 echter het standpunt in dat aanzienlijke vorderingen waren gemaakt en de meeste problemen waren opgelost wat de veilige haven betreft:

Op 24 juli 2013, na de onthullingen over Amerikaanse observatieprogramma's, gingen Duitse gegevensbeschermingsautoriteiten nog een stap verder door hun bezorgdheid te uiten dat de beginselen uit de rechtsbesluiten van de Commissie zeer waarschijnlijk worden geschonden[18]. Er zijn gevallen waarin sommige gegevensbeschermingsautoriteiten (bv. die van Bremen) een onderneming die persoonsgegevens doorgeeft aan providers uit de VS, hebben verzocht de gegevensbeschermingsautoriteit te laten weten of en hoe die providers voorkomen dat de nationale veiligheidsdienst daar toegang toe heeft. De Ierse gegevensbeschermingsautoriteit heeft meegedeeld dat zij recentelijk twee klachten heeft ontvangen over de veiligehavenregeling naar aanleiding van de verslaggeving over de observatieprogramma's van de Amerikaanse inlichtingendiensten, maar heeft geweigerd deze te onderzoeken omdat de doorgifte van persoonsgegevens naar een derde land aan de eisen van de Ierse wetgeving inzake gegevensbescherming voldeed. Na een soortgelijke klacht stelde de Luxemburgse gegevensbeschermingsautoriteit vast dat Microsoft en Skype de Luxemburgse wet inzake gegevensbescherming hadden nageleefd bij de doorgifte van gegevens naar de VS[19]. Het Ierse Hooggerechtshof heeft inmiddels echter een verzoek om rechterlijke toetsing ontvankelijk verklaard op grond waarvan het het niet-optreden van de Ierse toezichthouder voor gegevensbescherming in verband met de Amerikaanse observatieprogramma's zal beoordelen. Een van de twee klachten werd ingediend door een groep studenten, Europe v Facebook (EvF), die in Duitsland ook een soortgelijke klacht tegen Yahoo heeft ingediend, en wordt behandeld door de bevoegde gegevensbeschermingsautoriteiten.

Deze uiteenlopende reacties van gegevensbeschermingsautoriteiten op de onthullingen over de observatieprogramma's tonen het reële risico van de versnippering van de veiligehavenregeling aan en doen vragen rijzen met betrekking tot de mate waarin deze wordt gehandhaafd.

3. TRANSPARANTIE VAN HET PRIVACYBELEID VAN DEELNEMENDE ONDERNEMINGEN

Krachtens FAQ 6, die als bijlage is gevoegd bij de veiligehavenbeschikking (bijlage II), moeten ondernemingen die geïnteresseerd zijn in een certificering voor de veilige haven, het ministerie van Handel een beschrijving van het beleid inzake de bescherming van de persoonlijke levenssfeer verstrekken en deze publiek toegankelijk maken. Daarin moeten zij aangeven dat zij de privacybeginselen onderschrijven. Het vereiste om het **privacybeleid** van ondernemingen met een zelfcertificering en hun verklaring om de privacybeginselen te onderschrijven, **publiek toegankelijk te maken**, is essentieel voor de werking van de regeling.

Onvoldoende toegang tot het privacybeleid van dergelijke ondernemingen gaat ten koste van personen van wie persoonsgegevens worden verzameld en verwerkt, en kan een **inbreuk vormen op het beginsel van kennisgeving**. In dergelijke gevallen zijn de personen van wie de gegevens vanuit de EU worden doorgegeven, misschien niet op de hoogte van hun rechten, noch van de verplichtingen waaraan een onderneming met een zelfcertificering is onderworpen.

Bovendien brengt de verbintenis van ondernemingen om de privacybeginselen na te leven, **de bevoegdheid van de Federal Trade Commission teweeg om deze beginselen te handhaven** tegen ondernemingen in geval van niet-naleving als een oneerlijke of misleidende

---

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf

[18] Zie een resolutie van een Duitse conferentie van toezichthouders voor gegevensbescherming waarin wordt gesteld dat de inlichtingendiensten een enorme bedreiging vormen voor het dataverkeer tussen Duitsland en landen buiten Europa: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870

[19] Zie het persbericht van de Luxemburgse gegevensbeschermingsautoriteit van 18 november 2013.

praktijk. Een gebrek aan transparantie van ondernemingen in de VS maakt het toezicht door de Federal Trade Commission moeilijker en ondermijnt de doeltreffendheid van de handhaving.

In de loop der jaren heeft een aanzienlijk aantal ondernemingen met zelfcertificering, zijn privacybeleid niet openbaar gemaakt en/of geen publieke verklaring afgelegd ter onderschrijving van de privacybeginselen. In het verslag over de veilige haven van 2004 werd gewezen op de noodzaak voor het ministerie van Handel om **een actievere houding aan te nemen bij de controle van de naleving** van dit vereiste.

Vanaf 2004 heeft het ministerie van Handel **nieuwe informatie-instrumenten** ontwikkeld, gericht op het bijstaan van ondernemingen bij de vervulling van hun transparantieverplichtingen. De relevante informatie over de regeling kan worden geraadpleegd op de website van het ministerie van Handel over de veilige haven[20] waar ondernemingen ook hun privacybeleid kunnen uploaden. Het ministerie van Handel heeft gemeld dat ondernemingen van deze functie gebruik hebben gemaakt en hun privacybeleid op de website van het ministerie van Handel hebben gezet bij de aanvraag om tot de veilige haven toe te treden[21]. Bovendien heeft het ministerie van Handel in de periode 2009-2013 een reeks richtsnoeren gepubliceerd voor ondernemingen die aan de veilige haven wensen deel te nemen, zoals de "Guide to Self-Certification" (gids voor zelfcertificering) en de "Helpful Hints on Self-Certifying Compliance" (nuttige tips voor een correcte zelfcertificering)[22].

De mate waarin de transparantieverplichtingen worden nageleefd, varieert tussen ondernemingen. Bepaalde ondernemingen beperken zich tot de kennisgeving aan het ministerie van Handel van een beschrijving van hun privacybeleid als onderdeel van het zelfcertificeringsproces, maar de meeste ondernemingen maken hun privacybeleid openbaar toegankelijk op hun website, en uploaden dit niet alleen op de website van het ministerie van Handel. **Dat beleid wordt** echter **niet altijd op een consumentvriendelijke en gemakkelijk leesbare vorm gepresenteerd**. Hyperlinks naar privacybeleid werken niet altijd correct en verwijzen niet altijd naar de juiste webpagina's.

Uit de beschikking en de bijlagen daarbij vloeit voort dat het voorschrift dat ondernemingen hun privacybeleid publiek toegankelijk moeten maken, **meer inhoudt dan de loutere kennisgeving** van zelfcertificering bij het ministerie van Handel. De voorschriften inzake certificering die in de FAQs zijn vastgesteld, omvatten een beschrijving van het privacybeleid en transparante informatie over de plaats waar deze door het publiek kan worden geraadpleegd[23]. Verklaringen inzake het privacybeleid moeten duidelijk zijn en gemakkelijk toegankelijk voor het publiek. Zij dienen een hyperlink naar de website van het ministerie van Handel over de veilige haven te bevatten waarop alle "actuele" leden die bij de regeling zijn aangesloten, zijn opgesomd en een link naar de alternatieve geschillenbeslechter. Een aantal aan de regeling deelnemende ondernemingen heeft echter in de periode 2000-2013 niet aan deze vereisten voldaan. Tijdens werkcontacten met de Commissie in februari 2013 heeft het ministerie van Handel erkend dat mogelijk 10% van de gecertificeerde ondernemingen niet werkelijk hun privacybeleid met een bevestigende veiligehavenverklaring op hun respectieve websites heeft gezet.

Uit recente statistieken blijkt ook het aanhoudende probleem van **valse aanspraken op deelneming aan de veilige haven**. Ongeveer 10 % van de ondernemingen die beweren lid te

---

20 http://www.export.gov/SafeHarbour/

21 https://SafeHarbour.export.gov/list.aspx

22 De Guide is beschikbaar op de website van het programma: http://export.gov/SafeHarbour/ Helpful Hints: http://export.gov/SafeHarbour/eu/eg_main_018495.asp

23 Op 12 november 2013 heeft het ministerie van Handel bevestigd dat ondernemingen die over publieke websites beschikken en consumenten-, cliënten-, en bezoekersgegevens beheren, op hun website hun privacybeleid in overeenstemming met de veilige haven moeten publiceren (document: "U.S.-EU Cooperation to Implement the Safe Harbor Framework" van 12 november 2013).

zijn van de veilige haven, is niet opgenomen in de lijst van actuele bij regeling aangesloten leden die wordt opgesteld door het ministerie van Handel[24]. Dergelijke valse aanspraken komen zowel van ondernemingen die nooit aan de veilige haven hebben deelgenomen als van ondernemingen die ooit aangesloten waren bij de regeling, maar nadien hebben nagelaten bij het ministerie van Handel jaarlijks een nieuwe aanvraag voor zelfcertificering in te dienen. In dit geval blijven zij op de lijst van de veiligehavenwebsite staan, maar met de certificeringsstatus "niet actueel", hetgeen betekent dat de onderneming aangesloten is geweest bij de regeling en derhalve de verplichting heeft de reeds verwerkte gegevens te blijven beschermen. De Federal Trade Commission is bevoegd om in te grijpen in gevallen van misleidende praktijken en niet-naleving van de veiligehavenbeginselen (zie punt 5.1). Onduidelijkheid over de valse aanspraken tast de geloofwaardigheid van de regeling aan.

De Europese Commissie heeft het ministerie van Handel er tijdens regelmatige contacten in 2012 en 2013 attent op gemaakt dat het, om te voldoen aan de transparantieverplichtingen, niet volstaat dat ondernemingen alleen een beschrijving van hun privacybeleid ter beschikking stellen aan het ministerie van Handel. Verklaringen inzake het privacybeleid moeten voor het publiek toegankelijk worden gemaakt. Het ministerie van Handel werd ook verzocht om een **intensivering van zijn periodieke controles van de websites van de ondernemingen** na de verificatieprocedure die wordt uitgevoerd in het kader van de eerste zelfcertificeringsprocedure of de jaarlijkse hernieuwing daarvan en om actie te ondernemen tegen de ondernemingen die niet voldoen aan de vereisten inzake transparantie.

Als een eerste reactie op de bezorgdheid van de EU **heeft het ministerie van Handel vanaf maart 2013** voor een veiligehavenonderneming met een publieke website **de verplichting ingevoerd** om haar privacybeleid voor consumenten- of gebruikersgegevens direct beschikbaar te maken op haar publieke website. Tegelijkertijd is het ministerie van Handel begonnen met het melden aan alle ondernemingen van wie het privacybeleid nog geen link bevatte naar de veiligehavenwebsite van het ministerie van Handel, dat zij in een dergelijke link moeten voorzien, waardoor de officiële veiligehavenlijst en de website rechtstreeks toegankelijk worden voor consumenten die de website van een onderneming bezoeken. Hierdoor zullen de Europese betrokkenen onmiddellijk, zonder aanvullende opzoekingen op het internet, de bij het ministerie van Handel aangemelde verbintenissen van een onderneming kunnen verifiëren. Bovendien is het ministerie van Handel begonnen met het melden aan de ondernemingen dat de contactgegevens van hun onafhankelijke geschillenbeslechter in hun op het internet geplaatste privacybeleid moeten worden opgenomen[25].

Dit proces moet worden versneld om ervoor te zorgen dat alle gecertificeerde ondernemingen uiterlijk in maart 2014 (dat is de termijn voor de jaarlijkse hercertificering van ondernemingen, te rekenen vanaf de invoering van nieuwe voorschriften in maart 2013) aan de veiligehavenvoorschriften voldoen.

Niettemin blijft er bezorgdheid bestaan over de vraag of alle ondernemingen met zelfcertificering volledig voldoen aan de transparantievereisten. Het ministerie van Handel

---

[24] In september 2013 heeft de Australische consultant Galexia de valse aanspraken op lidmaatschap van de veilige haven in 2008 en 2013 vergeleken. De voornaamste bevinding was dat, parallel met de toename van het lidmaatschap van de veilige haven tussen 2008 en 2013 (van 1 109 tot 3 246), het aantal valse aanspraken is toegenomen van 206 tot 427. http://www.galexia.com/public/about/news/about_news-id225.html

[25] Tussen maart en september 2013 heeft het ministerie van Handel:
• aan 101 ondernemingen *die hun veilige haven-conforme privacybeleid reeds op de veiligehavenwebsite hadden geüpload,* gemeld dat zij hun privacybeleid ook op hun bedrijfswebsite moesten plaatsen;
• aan 154 ondernemingen die dat nog niet hadden gedaan, gemeld dat zij in hun privacybeleid een link naar de veiligehavenwebsite moesten opnemen;
• aan meer dan 600 ondernemingen gemeld dat zij in hun privacybeleid de contactgegevens van hun onafhankelijke geschillenbeslechter moesten opnemen.

zou grondiger moeten controleren en onderzoeken of de verbintenissen die bij de eerste zelfcertificering en bij de jaarlijkse hernieuwingen zijn aangegaan, worden nagekomen.

4. OPNAME VAN DE VEILIGEHAVENBEGINSELEN IN HET PRIVACYBELEID VAN ONDERNEMINGEN

Ondernemingen met een zelfcertificering moeten voldoen aan de in bijlage I bij de beschikking opgenomen privacybeginselen om de voordelen van de veilige haven te verkrijgen en te behouden.

In het verslag van 2004 heeft de Commissie vastgesteld dat een aanzienlijk aantal **ondernemingen de privacybeginselen van de veilige haven niet correct** in hun gegevensverwerkingsbeleid had opgenomen. Personen kregen bijvoorbeeld niet altijd duidelijke en transparante informatie over de doeleinden waarvoor hun gegevens werden verwerkt of kregen niet de mogelijkheid om zich te verzetten tegen de bekendmaking van hun gegevens aan een derde of tegen het gebruik ervan voor een doel dat niet verenigbaar is met de doeleinden waarvoor de gegevens oorspronkelijk waren verzameld. In haar verslag van 2004 vond de Commissie dat het ministerie van Handel proactiever moest zijn met betrekking tot de toegang tot de veilige haven en de bekendmaking van de beginselen[26].

Er is beperkte vooruitgang op dit gebied. Sinds 1 januari 2009 evalueert het ministerie van Handel het privacybeleid van elke onderneming die haar certificeringsstatus voor de veilige haven wil vernieuwen (hetgeen jaarlijks moet gebeuren), voorafgaand aan die hernieuwing. Die evaluatie is echter beperkt in omvang. Er vindt **geen volledige evaluatie plaats van de werkelijke praktijk** in de ondernemingen met een zelfcertificering, terwijl een dergelijke evaluatie de geloofwaardigheid van het zelfcertificeringsproces aanzienlijk zou vergroten.

Naar aanleiding van het verzoek van de Commissie om een strenger en meer systematisch toezicht door het ministerie van Handel op ondernemingen met een zelfcertificering, **wordt thans meer aandacht besteed aan nieuwe aanvragen**. Het aantal nieuwe aanvragen die niet werden aanvaard, maar werden teruggezonden naar de ondernemingen ter verbetering van het privacybeleid, is aanzienlijk toegenomen tussen 2010 en 2013: een verdubbeling voor ondernemingen die hercertificeren en een verdrievoudiging voor nieuwkomers bij de veilige haven[27]. Het ministerie van Handel heeft de Commissie verzekerd dat elke certificering of hercertificering pas kan worden voltooid wanneer het privacybeleid van de onderneming aan alle voorschriften voldoet, en in het bijzonder pas wanneer deze een bevestigende verbintenis bevat de betrokken reeks privacybeginselen van de veilige haven te onderschrijven en het privacybeleid publiek beschikbaar is. Een onderneming is verplicht om in de veiligehavenlijst aan te geven waar het betrokken beleid kan worden geraadpleegd. Op haar website moet ook duidelijk een alternatieve geschillenbeslechter worden aangewezen en een link worden opgenomen naar de zelfcertificering voor de veilige haven op de website van het ministerie van Handel. Naar schatting meer dan 30% van de veiligehavenleden verstrekt echter geen informatie over geschillenbeslechting in het privacybeleid op hun website[28].

Een meerderheid van de ondernemingen die het ministerie van Handel van de veiligehavenlijst heeft verwijderd, werd op uitdrukkelijk verzoek van de betrokken

[26] Zie bladzijde 8 van het verslag van 2004, SEC (2004) 1323.

[27] Volgens statistieken die het ministerie van Handel in september 2013 verstrekte, meldde dat ministerie in 2010 aan 18% (93) van de 512 ondernemingen die zich voor het eerst certificeerden en aan 16% (231) van de 1 417 ondernemingen die zich opnieuw certificeerden, dat zij verbeteringen dienden aan te brengen in hun privacybeleid en/of veiligehavenaanvragen. Naar aanleiding van de verzoeken van de Commissie om streng, grondig en systematisch onderzoek van alle aanvragen, had het ministerie van Handel tot half september 2013 56% (340) van de 602 ondernemingen die zich voor het eerst certificeerden en 27% (493) van de 1 809 ondernemingen die zich opnieuw certificeerden, verzocht om verbeteringen aan te brengen in hun privacybeleid.

[28] Verschijning van Chris Connolly (Galexia) voor het onderzoek van de LIBE-commissie van het Europees Parlement op 7 oktober 2013.

ondernemingen verwijderd (bv. gefuseerde of overgenomen ondernemingen, ondernemingen die hun bedrijfsactiviteiten hadden gewijzigd of stopgezet). Een kleiner aantal registraties van vervallen ondernemingen werd verwijderd wanneer de in de registraties opgegeven websites niet langer bleken te werken en de certificeringsstatus gedurende verscheidene jaren "niet actueel" was"[29]. Van belang is dat geen van deze verwijderingen lijkt te hebben plaatsgevonden omdat de controle van het ministerie van Handel tot de vaststelling leidde dat er nalevingsproblemen waren.

De registratie op de veiligehavenlijst dient als openbare kennisgeving en als registratie van de veiligehavenverbintenissen van een onderneming. **De verbintenis om de veiligehavenbeginselen te onderschrijven, is niet in de tijd beperkt** wat betreft de gegevens die zijn ontvangen tijdens de periode waarin de onderneming de voordelen van de veilige haven geniet, en de onderneming moet de beginselen blijven toepassen op dergelijke gegevens, zolang zij deze opslaat, gebruikt of bekendmaakt, ongeacht de reden waarom zij de veilige haven verlaat.

Met betrekking tot het aantal **veiligehavenaanvragers die niet slaagden voor de administratieve toetsing** door het ministerie van Handel en derhalve nooit zijn toegevoegd aan de veiligehavenlijst, geldt het volgende: **in 2010** werd slechts **6%** (33) van de 513 ondernemingen die zich voor het eerst registreerden, niet opgenomen in de veiligehavenlijst omdat zij niet voldeden aan de normen voor zelfcertificering van het ministerie van Handel. **In 2013** werd **12 %** (75) van de 605 ondernemingen die zich voor het eerst registreerden, niet opgenomen in de veiligehavenlijst omdat zij niet voldeden aan de normen voor zelfcertificering van het ministerie van Handel.

Als een minimumvereiste om de transparantie van het toezicht te vergroten, zou het ministerie van Handel op zijn website een lijst moeten opnemen van alle ondernemingen die van de veilige haven werden verwijderd en de redenen vermelden waarom de certificering niet is verlengd. Het label "niet actueel" op de lijst van veiligehavenondernemingen van het ministerie van Handel zou niet louter als informatie mogen worden beschouwd maar zou vergezeld moeten gaan van een **duidelijke waarschuwing** — zowel verbaal als grafisch — dat een onderneming op dat ogenblik niet aan de veiligehavenvereisten voldoet.

Bovendien voldoen sommige ondernemingen nog steeds niet volledig aan de veiligehavenbeginselen. Naast de transparantiekwestie die in punt 3 hierboven wordt behandeld, is het privacybeleid van ondernemingen met een zelfcertificering, dikwijls onduidelijk wat betreft de doeleinden waarvoor de gegevens worden verzameld, en het recht om te kiezen of gegevens al dan niet aan derde partijen kunnen worden bekendgemaakt; daardoor rijzen problemen inzake naleving van de privacybeginselen betreffende "kennisgeving" en "keuze". Kennisgeving en keuze zijn van cruciaal belang om ervoor te zorgen dat betrokkenen controle hebben over wat er gebeurt met hun persoonsgegevens.

De belangrijke eerste stap in het nalevingsproces, de opname van de privacybeginselen van de veilige haven in het privacybeleid van ondernemingen, is onvoldoende gewaarborgd. Het ministerie van Handel zou deze kwestie als een prioriteit moeten behandelen door een nalevingsmethodologie te ontwikkelen in de operationele praktijk van ondernemingen en hun interactie met klanten. **Er moet sprake zijn van een actieve follow-up door het ministerie van Handel van het effectief opnemen van de veiligehavenbeginselen in het privacybeleid van ondernemingen,** in plaats van de handhavingsmaatregelen te laten afhangen van klachten van personen.

[29] In december 2011 had het Amerikaanse ministerie van Handel 323 ondernemingen van de veiligehavenlijst verwijderd: 94 ondernemingen werden verwijderd omdat zij niet langer bedrijfsactiviteiten uitoefenden; 88 ondernemingen wegens fusie of overname, 95 op verzoek van de moederonderneming; 41 ondernemingen wegens herhaald nalaten om om hercertificering te verzoeken en 5 ondernemingen om diverse redenen.

5. HANDHAVING DOOR DE OVERHEID

Er zijn een aantal mechanismen beschikbaar voor een effectieve handhaving van de veiligehavenregeling en om personen verhaalsmogelijkheden te bieden in gevallen waarin de bescherming van hun persoonsgegevens wordt aangetast door de niet-naleving van de beginselen.

Volgens het "handhavingsbeginsel" moet het privacybeleid van organisaties met zelfcertificering doeltreffende handhavingsmechanismen bevatten. Volgens het handhavingsbeginsel, zoals nader uiteengezet in FAQs 11, 5 en 6, kan aan dit vereiste worden voldaan door **onafhankelijke verhaalmechanismen** te onderschrijven ten aanzien waarvan publiek is verklaard dat er sprake is van de bevoegdheid om kennis te nemen van individuele klachten inzake niet-naleving van de beginselen. Dit kan ook worden bereikt doordat de organisatie zich ertoe verbindt om met het **gegevensbeschermingspanel van de EU** samen te werken[30]. Bovendien vallen ondernemingen met zelfcertificering onder de bevoegdheid van de Federal Trade Commission overeenkomstig artikel 5 van de Federal Trade Commission Act, waarin oneerlijke of misleidende daden of praktijken in of in verband met de handel worden verboden[31].

In het verslag van 2004 werd bezorgdheid geuit over de handhaving van de veiligehavenregeling, meer bepaald over het feit dat de Federal Trade Commission proactiever moest zijn bij het openen van onderzoeken en om burgers bewust te maken van hun rechten. Een andere bron van zorg was het gebrek aan duidelijkheid met betrekking tot de bevoegdheden van de Federal Trade Commission inzake de handhaving van de beginselen wat personeelsgegevens betreft.

Het orgaan om verhaal te halen inzake personeelsgegevens, het gegevensbeschermingspanel van de EU, heeft één klacht ontvangen over personeelsgegevens[32]. Uit het ontbreken van klachten mogen echter geen conclusies worden getrokken over de werking van de regeling in zijn geheel. Er moeten ambtshalve controles worden ingevoerd op de naleving door ondernemingen om na te gaan of zij hun verbintenissen inzake gegevensbescherming daadwerkelijk ten uitvoer leggen. Gegevensbeschermingsautoriteiten in de EU moeten ook maatregelen nemen om de bekendheid van het panel te bevorderen.

Er werd gewezen op problemen in verband met de wijze waarop alternatieve verhaalmechanismen als handhavingsinstanties werken. Een aantal van deze instanties beschikt niet over passende middelen om gevallen van niet-naleving van de beginselen te verhelpen. Deze tekortkoming moet worden aangepakt.

---

30 Het gegevensbeschermingspanel van de EU is een orgaan dat bevoegd is voor het onderzoeken en het afhandelen van klachten van particulieren wegens vermeende inbreuken op de veiligehavenbeginselen door een Amerikaanse onderneming die bij de veilige haven is aangesloten. Ondernemingen die de veiligehavenbeginselen certificeren, moeten ervoor kiezen hetzij een onafhankelijk verhaalmechanisme te onderschrijven, hetzij samen te werken met het gegevensbeschermingspanel van de EU om problemen op te lossen die voortvloeien uit de niet-naleving van de veiligehavenbeginselen. Samenwerking met het gegevensbeschermingspanel van de EU is evenwel verplicht wanneer de Amerikaanse onderneming personeelsgegevens verwerkt die vanuit de EU zijn doorgegeven in het kader van een arbeidsverhouding. Indien de onderneming zich ertoe verbindt samen te werken met het EU-panel, moet zij zich er ook toe verbinden zich te schikken naar eventuele adviezen van het EU-panel wanneer dat van oordeel is dat de onderneming specifieke maatregelen moet nemen om de veiligehavenbeginselen na te leven, met inbegrip van corrigerende of compenserende maatregelen.

31 Het ministerie van Vervoer beschikt over een soortgelijke bevoegdheid ten aanzien van luchtvaartmaatschappijen krachtens titel 49, artikel 41712 van de United States Code.

32 De klacht was afkomstig van een Zwitserse staatsburger en werd derhalve door het gegevensbeschermingspanel van de EU verwezen naar de Zwitserse autoriteit voor gegevensbescherming (de VS hebben een afzonderlijke veiligehavenregeling voor Zwitserland).

5.1. Federal Trade Commission

De Federal Trade Commission kan handhavingsmaatregelen nemen in geval van schendingen van de veiligehavenverbintenissen die ondernemingen aangaan. Toen de veiligehavenregeling werd ingevoerd, verbond de Federal Trade Commission zich ertoe alle verwijzingen van autoriteiten van EU-lidstaten prioritair te onderzoeken[33]. Aangezien er tijdens de eerste tien jaar van de regeling geen klachten waren ontvangen, besloot de Federal Trade Commission op zoek te gaan naar schendingen van de veilige haven in elk onderzoek dat zij uitvoerde inzake privacy en gegevensbeveiliging. Sinds 2009 heeft de Federal Trade Commission 10 handhavingsmaatregelen genomen tegen ondernemingen op basis van schendingen van de veilige haven. Deze maatregelen hebben met name geleid tot schikkingsbevelen — op straffe van aanzienlijke boetes — houdende een verbod op onjuiste verklaringen over privacy, met inbegrip van de naleving van de veiligehavenregeling, waarbij uitvoerige privacyprogramma's en audits voor de duur van 20 jaar werden opgelegd. De ondernemingen moeten onafhankelijke beoordelingen van hun privacyprogramma's aanvaarden wanneer de Federal Trade Commission daar om verzoekt. Over deze beoordelingen wordt regelmatig verslag uitgebracht aan de Federal Trade Commission. De bevelen van de Federal Trade Commission verbieden deze ondernemingen ook hun privacypraktijken en hun deelname aan de veilige haven of soortgelijke privacyregelingen verkeerd voor te stellen. Dit was bijvoorbeeld het geval voor de onderzoeken van de Federal Trade Commission tegen Google, Facebook en MySpace[34]. In 2012 stemde Google in met de betaling van een boete van 22,5 miljoen als schikking de beschuldigingen dat het een consent order had geschonden. In alle privacy-onderzoeken gaat de Federal Trade Commission ambtshalve na of er sprake is van een schending van de veilige haven.

De Federal Trade Commission heeft onlangs haar verklaringen en verbintenis opnieuw bevestigd om verwijzingen van ondernemingen die inzake privacy zelfregulerend optreden en van EU-lidstaten, die beweren dat een onderneming de veiligehavenbeginselen heeft geschonden, prioritair te zullen onderzoeken[35]. De laatste drie jaar heeft de Federal Trade Commission slechts enkele verwijzingen van Europese gegevensbeschermingsautoriteiten ontvangen.

De voorbije maanden startte de ontwikkeling van de trans-Atlantische samenwerking tussen autoriteiten voor gegevensbescherming. De Federal Trade Commission ondertekende bijvoorbeeld op 26 juni 2013 samen met het Ierse Office of the Data Protection Commissioner een memorandum van overeenstemming over wederzijdse bijstand inzake de handhaving van het recht ter bescherming van persoonsgegevens in de private sector. Het memorandum voorziet in een kader voor versterkte, beter gestroomlijnde en meer doeltreffende samenwerking op het gebied van handhaving in privacykwesties[36].

In augustus 2013 kondigde de Federal Trade Commission aan dat de controles van ondernemingen die grote databanken met persoonsgegevens controleren, verder zou worden

---

33 Zie bijlage V bij Beschikking 2000/520/EG van de Commissie van 26 juli 2000.

34 In de periode 2009-2012 heeft de Federal Trade Commission tien handhavingsmaatregelen genomen inzake veiligehavenverbintenissen: FTC v. Javian Karnani, en Balls of Kryptonite, LLC (2009), World Innovators, Inc. (2009), Expat Edge Partners, LLC (2009), Onyx Graphics, Inc. (2009), Directors Desk LLC (2009), Progressive Gaitways LLC (2009), Collectify LLC (2009), Google Inc. (2011), Facebook, Inc. (2011), Myspace LLC (2012). Zie: "Federal Trade Commission of Safe Harbour Commitments": http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf Zie ook: "Case Highlights": http://business.ftc.gov/us-eu-Safe-Harbour-framework. In de meeste van deze gevallen ging het om problemen met ondernemingen die de veilige haven hebben onderschreven, maar zich vervolgens als lid bleven uitgeven zonder hun certificering jaarlijks te hernieuwen.

35 Deze verbintenis werd opnieuw bevestigd tijdens een bijeenkomst van Commissioner Julie Brill van de Federal Trade Commission met gegevensbeschermingsautoriteiten uit de EU (Groep artikel 29) in Brussel op 17 april 2013.

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n

versterkt. Zij heeft ook een portaal opgericht waar consumenten een klacht inzake privacy kunnen indienen ten aanzien van een onderneming uit de VS[37].

De Federal Trade Commission zou ook meer inspanningen moeten leveren om valse aanspraken op het lidmaatschap van de veilige haven te onderzoeken. Een onderneming die op zijn website beweert te voldoen aan de veiligehavenvoorschriften, maar die niet als "actueel" lid voorkomt op de lijst van het ministerie van Handel, misleidt consumenten en maakt misbruik van hun vertrouwen. Valse aanspraken tasten de geloofwaardigheid van het systeem als geheel aan en moeten daarom onmiddellijk van de websites van de ondernemingen worden verwijderd. De ondernemingen zouden moeten gebonden zijn door een afdwingbare verplichting de consumenten niet te misleiden. De Federal Trade Commission moet blijven zoeken naar valse aanspraken op deelname aan de veilige haven, zoals die in de zaak *Karnani,* waarin de Federal Trade Commission een Californische website sloot omdat daarop valselijk een veiligehavenregistratie werd vermeld en waarbij sprake was van frauduleuze e-handelspraktijken gericht op Europese consumenten[38].

Op 29 oktober 2013 kondigde de Federal Trade Commission aan dat zij in de "afgelopen maanden talrijke onderzoeken had geopend inzake de veilige haven" en dat "in de komende maanden" op dit gebied nog meer handhavingsmaatregelen konden worden verwacht. De Federal Trade Commission bevestigde ook "dat zij vastberaden zou zoeken naar manieren om haar doeltreffendheid te verbeteren en zou blijven uitkijken naar belangrijke initiatieven, zoals de klacht die een Europese consumentenadvocaat de afgelopen maand indiende inzake een groot aantal vermeende veiligehavenschendingen"[39]. De instelling verbond zich er ook toe "systematisch toezicht te houden op de naleving van veiligehavenbevelen, zoals met alle bevelen gebeurt"[40].

Op 12 november 2013 deelde de Federal Trade Commission de Europese Commissie mee dat "**indien een onderneming in haar privacybeleid veiligehavenbescherming belooft, het nalaten om een registratie te verrichten of te behouden, dit op zich de betrokken onderneming waarschijnlijk niet zal vrijwaren tegen handhaving van die veiligehavenverbintenissen door de Federal Trade Commission**"[41].

In november 2013 heeft het ministerie van Handel de Europese Commissie meegedeeld dat het "om ervoor te helpen zorgen dat ondernemingen geen valse aanspraken maken op deelname aan de veilige haven, een procedure zal starten waarbij één maand vóór de hercertificering contact zal worden opgenomen met veiligehavendeelnemers om de stappen te beschrijven die zij moeten volgen in het geval zij niet opnieuw willen certificeren". **Het ministerie van Handel "zal deze categorie ondernemingen aanmanen** alle verwijzingen naar deelname aan de veilige haven te verwijderen uit hun privacybeleid en websites, met inbegrip van het gebruik van het certificeringsmerkteken van het ministerie, **en hen duidelijk meedelen dat het nalaten daarvan kan leiden tot handhavingsmaatregelen van het ministerie**"[42].

Om valse aanspraken op deelname aan de veilige haven tegen te gaan, zou het privacybeleid op de websites van ondernemingen met een zelfcertificering steeds een link moeten bevatten naar de veiligehavenwebsite van het ministerie van Handel, waar alle "actuele" leden van de

---

37 Consumenten kunnen hun klachten indienen via de Federal Trade Commission Complaint Assistant (https://www.ftccomplaintassistant.gov/) en internationale consumenten kunnen een klacht indienen via econsumer.gov (http://www.econsumer.gov).

38 http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf

39 http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf en http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf

40 Brief van de voorzitter van de Federal Trade Commission, Edith Ramirez aan vicevoorzitter Viviane Reding.

41 Brief van de voorzitter van de Federal Trade Commission, Edith Ramirez aan vicevoorzitter Viviane Reding.

42 "U.S.-EU Cooperation to Implement the Safe Harbor Framework", 12 november 2013.

regeling zijn vermeld. Op die manier zullen de Europese betrokkenen onmiddellijk, zonder extra zoekopdrachten, kunnen verifiëren of een onderneming is aangesloten bij de veilige haven. In maart 2013 is het ministerie van Handel begonnen met ondernemingen daarom te verzoeken, maar dit proces zou moeten worden geïntensiveerd.

De voortdurende controle en daaruit voortvloeiende handhaving door de Federal Trade Commission van de effectieve naleving van de veiligehavenbeginselen — naast de maatregelen van het ministerie van Handel zoals hierboven onder de aandacht gebracht — blijft een belangrijke prioriteit voor het waarborgen van de correcte en efficiënte werking van de regeling. Er is vooral behoefte aan meer **ambtshalve controles van en onderzoeken naar het naleven** van de veiligehavenbeginselen **door ondernemingen**. Klachten bij de Federal Trade Commission over inbreuken moeten ook verder worden vergemakkelijkt.

5.2. Het EU-gegevensbeschermingspanel

Het EU-gegevensbeschermingspanel is een orgaan dat in het kader van de veiligehavenbeschikking is opgericht. Het is bevoegd voor het onderzoek van klachten die door personen zijn ingediend inzake persoonsgegevens die zijn verzameld in het kader van een arbeidsverhouding, alsook voor zaken betreffende gecertificeerde ondernemingen die deze optie voor geschillenbeslechting hebben gekozen in het kader van de veilige haven (53% van alle ondernemingen). Het panel is samengesteld uit vertegenwoordigers van diverse gegevensbeschermingsautoriteiten uit de EU.

Tot op heden heeft het panel vier klachten ontvangen (twee in 2010 en twee in 2013). De twee klachten in 2010 heeft het doorverwezen naar nationale gegevensbeschermingsautoriteiten (Verenigd Koninkrijk en Zwitserland). De derde en vierde klacht worden momenteel onderzocht. Het kleine aantal klachten kan worden verklaard door het feit dat de bevoegdheden van het panel, zoals eerder gezegd, hoofdzakelijk beperkt zijn tot een bepaald type gegevens.

Het beperkt aantal zaken zou ook deels te wijten kunnen zijn aan de beperkte bekendheid van het panel. In 2004 heeft de Commissie de informatie over het panel meer zichtbaar gemaakt op haar website[43].

Om beter gebruik te kunnen maken van het panel, zouden ondernemingen in de VS die ervoor hebben gekozen om met het panel samen te werken en zijn besluiten na te leven, voor sommige of alle categorieën persoonsgegevens die onder hun respectieve zelfcertificeringen vallen, dat duidelijk en opvallend in hun verbintenissen inzake privacybeleid moeten aangeven, zodat het ministerie van Handel dit aspect kan onderzoeken. De websites van alle gegevensbeschermingsautoriteiten uit de EU zouden een aparte pagina moeten hebben over de veiligehavenregeling om deze beter bekend te maken bij Europese ondernemingen en betrokkenen.

5.3. Betere handhaving

De zwakke punten in de transparantie en de zwakke punten in de handhaving die hierboven werden vastgesteld, leiden tot bezorgdheid bij Europese ondernemingen wat betreft de

[43] Ingevolge het verslag van 2004 werd op de website van de Commissie (DG Justitie) een toelichting gepubliceerd in de vorm van vragen en antwoorden van het EU-gegevensbeschermingspanel met het doel de kennis van burgers over het panel te vergroten en hen te helpen een klacht in te dienen wanneer zij van oordeel zijn dat hun persoonsgegevens in strijd met de veilige haven zijn verwerkt: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf
Het standaardformulier voor klachten is beschikbaar op http://ec.europa.eu/justice/policies/privacy/docs/adequacy/complaint_form_en.pdf

negatieve gevolgen van de veiligehavenregeling voor het concurrentievermogen van Europese bedrijven. Wanneer een Europese onderneming concurreert met een Amerikaanse onderneming die in het kader van de veilige haven handelt, maar in de praktijk de beginselen ervan niet toepast, heeft de Europese onderneming een concurrentieel nadeel ten opzichte van de Amerikaanse onderneming.

Voorts is de Federal Trade Commission bevoegd met betrekking tot oneerlijke of misleidende handelingen of praktijken "in of in verband met de handel". Artikel 5 van de Federal Trade Commission Act voorziet in uitzonderingen op de bevoegdheid van de Federal Trade Commission inzake oneerlijke of misleidende handelingen of praktijken ten aanzien van onder meer **telecommunicatie**. Aangezien zij niet onder de handhaving door de Federal Trade Commission vallen, mogen telecomondernemingen niet deelnemen aan de veilige haven. Gelet op de toenemende convergentie van technologieën en diensten zijn echter veel van hun directe concurrenten in de ICT-sector in de VS lid van de veilige haven. De uitsluiting van telecomondernemingen van de uitwisseling van gegevens in het kader van de veilige haven is een punt van zorg voor sommige Europese telecomoperatoren. Volgens de European Telecommunications Network Operators' Association (ETNO, Europese vereniging van exploitanten van telecommunicatienetwerken) "is dit duidelijk in strijd met het belangrijkste argument van de telecomoperatoren betreffende de noodzaak van een gelijk speelveld"[44].

6. VERSTERKING VAN DE VEILIGE HAVENBEGINSELEN

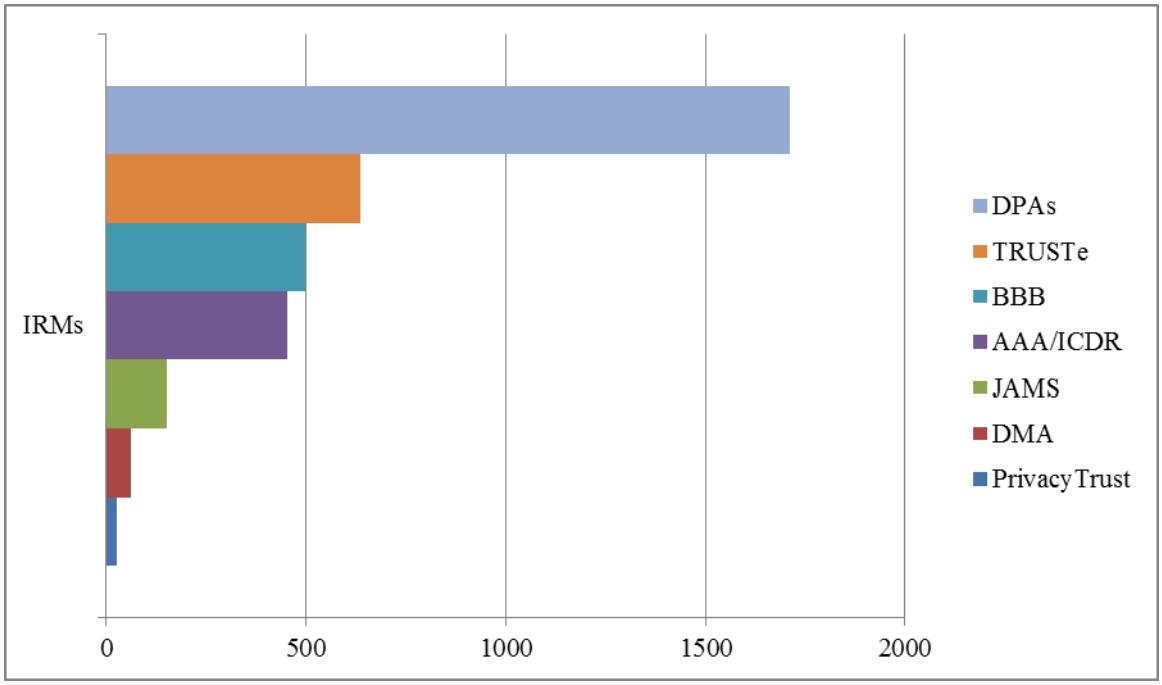
6.1. Alternatieve geschillenbeslechting

Het handhavingsbeginsel vereist dat er sprake is van "**direct beschikbare en betaalbare verhaalmechanismen** voor het onderzoek en de afhandeling van klachten en geschillen van particulieren". Te dien einde voorziet de veiligehavenregeling in een systeem van alternatieve geschillenbeslechting door een onafhankelijke derde partij[45] om snel oplossingen te vinden voor burgers. De drie belangrijkste instanties met verhaalmechanismen zijn het EU-gegevensbeschermingspanel, BBB (Better Business Bureaus) en TRUSTe.

---

44 In de "ETNO considerations" (opmerkingen van de ETNO) die de diensten van de Commissie op 4 oktober 2013 ontvingen, gaat het ook over 1) de definitie van persoonsgegevens in de veilige haven, 2) het gebrek aan controle op de veilige haven, 3) en het feit dat "Amerikaanse ondernemingen met veel minder beperkingen gegevens kunnen doorgeven dan hun Europese tegenhangers", hetgeen "een duidelijke discriminatie van Europese ondernemingen inhoudt en het concurrentievermogen van Europese ondernemingen aantast". Op grond van de veiligehavenregeling moeten organisaties die informatie bekendmaken aan een derde, het kennisgevingsbeginsel en het keuzebeginsel toepassen. Wanneer een organisatie informatie wil doorgeven aan een derde die als haar vertegenwoordiger optreedt, mag dit indien zij zich er eerst van vergewist dat deze derde de veiligehavenbeginselen onderschrijft, dan wel of de richtlijn of een andere vaststelling van gepastheid op hem van toepassing is, of indien zij een schriftelijke overeenkomst met deze derde aangaat waarin zij eist dat deze derde ten minste dezelfde bescherming van de persoonlijke levenssfeer biedt als de desbetreffende veiligehavenbeginselen bieden.

45 EU-Richtlijn 2013/11/EU betreffende alternatieve beslechting van consumentengeschillen onderstreept het belang van onafhankelijke, onpartijdige, transparante, doeltreffende, snelle en billijke procedures voor alternatieve geschillenbeslechting.



Het gebruik van alternatieve geschillenbeslechting is sinds 2004 toegenomen en het ministerie van Handel heeft de controle op Amerikaanse alternatieve geschillenbeslechters versterkt om ervoor te zorgen dat de informatie die zij verstrekken over de klachtenprocedure, duidelijk, toegankelijk en begrijpelijk is. De doeltreffendheid van dit systeem moet echter nog worden bewezen aangezien er tot nog toe nog maar een beperkt aantal zaken is behandeld[46].

Hoewel het ministerie van Handel erin geslaagd is de door de alternatieve geschillenbeslechters in rekening gebrachte vergoedingen te verlagen, vragen nog steeds twee van de zeven grote alternatieve geschillenbeslechters een vergoeding van burgers die een klacht indienen[47]. Het gaat om de alternatieve geschillenbeslechters die door ongeveer 20% van de veiligehavenondernemingen worden gebruikt. Deze ondernemingen hebben een alternatieve geschillenbeslechter geselecteerd die consumenten een vergoeding in rekening brengt voor het indienen van een klacht. Dergelijke praktijken zijn niet in overeenstemming met het handhavingsbeginsel van de veilige haven die personen recht geeft op toegang tot "direct beschikbare en betaalbare onafhankelijke verhaalmechanismen". In de Europese Unie is toegang tot een onafhankelijke geschillenbeslechtingsdienst, aangeboden door het EU-gegevensbeschermingspanel, kosteloos voor alle betrokkenen.

[46] Een belangrijke aanbieder ("TRUSTe") heeft bijvoorbeeld gemeld dat hij in 2010 881 verzoeken had ontvangen, maar dat slechts drie daarvan ontvankelijk en gegrond werden verklaard, en ertoe hebben geleid dat de betrokken onderneming haar privacybeleid en website moest veranderen. In 2011 bedroeg het aantal klachten 879 en moest in één geval de onderneming haar privacybeleid wijzigen. Volgens het ministerie van Handel heeft het merendeel van de klachten bij alternatieve geschillenbeslechting betrekking op verzoeken van consumenten, bijvoorbeeld gebruikers die hun paswoord waren vergeten en dit niet via het internet konden verkrijgen. Op verzoek van de Commissie heeft het ministerie van Handel nieuwe rapportagecriteria ontwikkeld voor statistieken die door alle alternatieve geschillenbeslechters moeten worden gebruikt. De criteria maken onderscheid tussen louter verzoeken enerzijds en klachten anderzijds en zij verstrekken duidelijkheid over het type van de ontvangen klachten. Over deze nieuwe criteria dient echter nog verder overleg plaats te vinden om ervoor te zorgen dat nieuwe statistieken in 2014 betrekking hebben op alle alternatieve geschillenbeslechters, vergelijkbaar zijn en belangrijke informatie aanreiken om de doeltreffendheid van het verhaalmechanisme te beoordelen.

[47] Het International Centre for Dispute Resolution / American Arbitration Association (ICDR/AAA), brengt 200 dollar en JAMS 250 dollar in rekening als “filing fee”. Het ministerie van Handel heeft de Commissie ervan in kennis gesteld dat zij had samengewerkt met de AAA, de duurste geschillenbeslechter voor individuele personen, om een specifiek programma voor de veilige haven te ontwikkelen dat de kosten voor consumenten verminderde van verschillende duizenden dollars tot een forfaitair bedrag van 200 dollar.

Op 12 november 2013 bevestigde het ministerie van Handel dat "het de privacy van Europese burgers zou blijven verdedigen en met de alternatieve geschillenbeslechters zou blijven samenwerken met het oog op een eventuele verdere daling van hun tarieven".

Wat sancties betreft, beschikken niet alle aanbieders van alternatieve geschillenbeslechting over de nodige instrumenten om een einde te maken aan situaties waarin de privacybeginselen niet worden nageleefd. Bovendien is de bekendmaking van geconstateerde gevallen van niet-naleving niet opgenomen in de sancties en maatregelen van alle alternatieve geschillenbeslechters.

Alternatieve geschillenbeslechters zijn ook verplicht om zaken naar de Federal Trade Commission te verwijzen wanneer een onderneming zich niet aan de uitkomst van een alternatieve geschillenbeslechtingsprocedure conformeert, of het besluit van de alternatieve geschillenbeslechter verwerpt, zodat de Federal Trade Commission de zaak kan toetsen en onderzoeken en indien nodig handhavingsmaatregelen nemen. Er zijn tot op heden echter nog geen zaken door een alternatieve geschillenbeslechter naar de Federal Trade Commission verwezen wegens niet-nakoming[48].

Alternatieve geschillenbeslechters bieden op hun websites lijsten aan van ondernemingen (deelnemers geschillenbeslechting) die gebruik maken van hun diensten. Dit maakt het de consument mogelijk om — in geval van een geschil met een onderneming — gemakkelijk na te gaan of een individu een klacht kan indienen bij een bepaalde geschillenbeslechter. Zo biedt de geschillenbeslechter BBB bijvoorbeeld een lijst aan van alle ondernemingen die onder het geschillenbeslechtingssysteem van BBB vallen. Talrijke ondernemingen beweren echter onder een specifiek geschillenbeslechtingssysteem te vallen, maar zijn niet opgenomen in de lijst van deelnemers aan het geschillenbeslechtingssysteem van de betrokken geschillenbeslechter[49].

Procedures voor alternatieve geschillenbeslechting moeten gemakkelijk toegankelijk, onafhankelijk en betaalbaar zijn voor burgers. Een betrokkene moet een klacht kunnen indienen zonder buitensporige beperkingen. Alle instellingen voor alternatieve geschillenbeslechting zouden op hun websites statistieken moeten publiceren over de behandelde klachten en specifieke informatie over de uitkomst daarvan. Ten slotte zouden instellingen voor alternatieve geschillenbeslechting verder gecontroleerd moeten worden om ervoor te zorgen dat de informatie die zij verstrekken over de procedure en over de manier waarop een klacht kan worden ingediend, duidelijk en begrijpelijk is, zodat de geschillenbeslechting een doeltreffend en betrouwbaar mechanisme wordt dat tot resultaten leidt. In dit verband moet er ook op worden gewezen dat de bekendmaking van geconstateerde gevallen van niet-naleving moet worden opgenomen in de reeks verplichte sancties van alternatieve geschillenbeslechters.

6.2. Verdere doorgifte

Vanwege de exponentiële groei van gegevensstromen moet worden gezorgd voor de blijvende bescherming van persoonsgegevens in alle stadia van de verwerking daarvan, met name wanneer gegevens door een onderneming die aan de veilige haven deelneemt worden doorgegeven aan een **derde verwerker**. Daarom heeft de behoefte aan een betere handhaving

[48] Zie FAQ 11.

[49] Voorbeelden: Amazon heeft het ministerie van Handel meegedeeld dat het BBB als geschillenbeslechter gebruikt. Amazon staat echter niet op de lijst van deelnemers aan de geschillenbeslechting van BBB. Vice versa staat Arsalon Technologies (www.arsalon.net), een aanbieder van cloud hosting, op de lijst veiligehavengeschillenbeslechting van BBB, maar de onderneming is geen actueel lid van de veilige haven (situatie op 1 oktober 2013). BBB, TRUSTe en andere alternatieve geschillenbeslechters zouden dergelijke aanspraken op certificering moeten verwijderen of corrigeren. Zij zouden moeten gebonden zijn door een afdwingbare verplichting om alleen ondernemingen te certificeren die deel uitmaken van de veilige haven.

van de veilige haven niet alleen betrekking op de deelnemers van de veilige haven, maar ook op subcontractanten.

Verdere doorgifte van gegevens aan een derde die als vertegenwoordiger van een onderneming optreedt, is mogelijk op grond van de veilige havenregeling indien de onderneming – die deelneemt aan de veiligehavenregeling – zich ervan "vergewist dat deze derde de veiligehavenbeginselen onderschrijft, dan wel of de richtlijn of een andere vaststelling van gepastheid op hem van toepassing is, of indien zij een schriftelijke overeenkomst met deze derde aangaat waarin zij eist dat deze derde ten minste dezelfde bescherming van de persoonlijke levenssfeer biedt als de veiligehavenbeginselen bieden"[50]. Van een aanbieder van clouddiensten bijvoorbeeld verlangt het ministerie van Handel dat hij een overeenkomst sluit, ook al is hij "veilige haven-conform" is en ontvangt hij persoonsgegevens voor verwerking[51]. Deze regel is echter niet duidelijk in bijlage II bij de veiligehavenbeschikking.

Aangezien het beroep op onderaannemers in de afgelopen jaren aanzienlijk is toegenomen, met name in de context van cloudcomputing, zou een veiligehavenonderneming bij het sluiten van een dergelijke overeenkomst het ministerie van Handel daarvan kennis moeten geven en verplicht moeten worden de privacywaarborgen publiek toegankelijk te maken[52].

De drie hierboven vermelde kwesties, het mechanisme voor alternatieve geschillenbeslechting, versterkt toezicht en verdere doorgifte van gegevens zouden verder moeten worden verduidelijkt.

7. TOEGANG TOT GEGEVENS DIE ZIJN DOORGEGEVEN IN HET KADER VAN DE VEILIGEHAVENREGELING

In de loop van 2013 heeft informatie over de schaal en de omvang van Amerikaanse observatieprogramma's vragen doen rijzen over de continuïteit van de bescherming van persoonsgegevens die rechtmatig aan de VS zijn doorgegeven in het kader van de veilige havenregeling. Alle ondernemingen die betrokken zijn bij het PRISM-programma en die de autoriteiten van de VS toegang verlenen tot in de VS opgeslagen en verwerkte gegevens, lijken bijvoorbeeld gecertificeerd te zijn in het kader van de veilige haven. Dit heeft van de veilige haven een van de kanalen gemaakt waarlangs de Amerikaanse inlichtingendiensten toegang hadden tot persoonsgegevens die oorspronkelijk in de EU waren verwerkt.

In bijlage 1 bij de veiligehavenbeschikking is bepaald dat de naleving van de privacybeginselen kan worden beperkt wanneer dat gerechtvaardigd is om aan de eisen van de nationale veiligheid, het algemeen belang en rechtshandhaving te voldoen of op grond van wettelijke of bestuursrechtelijke bepalingen of rechtspraak. Beperkingen en restricties op het genot van fundamentele rechten zijn slechts geldig wanneer zij strikt worden uitgelegd. Zij moeten zijn opgenomen in voor het publiek toegankelijke wetgeving en noodzakelijk en evenredig zijn in een democratische samenleving. In de veiligehavenbeschikking wordt met name gespecificeerd dat dergelijke beperkingen slechts mogelijk zijn "**voor zover dit nodig**

[50] Zie Beschikking 2000/520/EG van de Commissie, blz. 7 (verdere doorgifte).

[51] Zie: "Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing": http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf

[52] Deze opmerkingen hebben betrekking op cloudaanbieders die geen deel uitmaken van de veilige haven. Volgens de consultant Galexia nemen nogal wat aanbieders van clouddiensten deel aan de veiligehavenregeling (en leven ze deze ook na). Aanbieders van clouddiensten hebben in het algemeen verschillende lagen van privacybescherming, waarbij dikwijls directe contracten met cliënten en een overkoepelend privacybeleid worden gecombineerd. Op één of twee belangrijke uitzonderingen na, leven aanbieders van clouddiensten in de veilige haven de belangrijkste bepalingen inzake geschillenbeslechting en handhaving na. Op de lijst van valse aanspraken op deelname aan de veilige haven bevinden zich thans geen grote aanbieders van clouddiensten." (verschijning van Chris Connolly van Galexia voor het onderzoek van de LIBE-commissie inzake "Grootschalig elektronisch toezicht op EU-burgers").

is" om aan de eisen van de nationale veiligheid, het algemeen belang en rechtshandhaving te voldoen[53]. Hoewel de veiligehavenregeling de mogelijkheid biedt tot bij wijze van uitzondering verwerken van gegevens met het oog op de nationale veiligheid, het algemeen belang en rechtshandhaving, was de grootschalige toegang door inlichtingendiensten tot gegevens die aan de VS zijn doorgegeven in het kader van commerciële transacties niet te voorzien ten tijde van de invoering van de veilige haven.

Bovendien zou het ministerie van Handel om redenen van transparantie en rechtszekerheid aan de Europese Commissie elke wet of overheidsregeling moeten melden die afbreuk kan doen aan de naleving van de veiligehavenbeginselen[54]. Het gebruik van uitzonderingen moet zorgvuldig worden gecontroleerd en de uitzonderingen mogen niet worden gebruikt op een manier die leidt tot ondermijning van de bescherming die door de **beginselen** wordt geboden[55]. Vooral de grootschalige toegang van VS-autoriteiten tot gegevens die worden verwerkt door veiligehavenondernemingen met zelfcertificering houdt het gevaar in dat de vertrouwelijkheid van elektronische communicatie wordt ondermijnd.

7.1. Evenredigheid en noodzakelijkheid

Zoals blijkt uit de bevindingen van de EU-VS ad hoc-werkgroep voor gegevensbescherming, maken een aantal rechtsgrondslagen grootschalige verzameling en verwerking van persoonsgegevens mogelijk die is opgeslagen of anderszins verwerkt door in de VS gevestigde ondernemingen. Het kan gaan om gegevens die eerder vanuit de EU aan de VS werden doorgegeven in het kader van de veiligehavenregeling, en dit doet de vraag rijzen of de veiligehavenbeginselen nog steeds worden nageleefd. Het grootschalige karakter van deze programma's kan tot gevolg hebben dat meer gegevens die in het kader van de veilige haven zijn doorgegeven, door de Amerikaanse autoriteiten worden geraadpleegd en verder verwerkt dan strikt noodzakelijk is voor en evenredig is met de bescherming van de nationale veiligheid, zoals de uitzondering waarin de veiligehavenbeschikking voorziet, bepaalt.

7.2. Beperkingen en rechtsmiddelen

Zoals blijkt uit de bevindingen van de EU-VS ad hoc-werkgroep voor gegevensbescherming, zijn de waarborgen waarin het recht van de VS voorziet, in de meeste gevallen beschikbaar voor VS-burgers of legaal in de VS verblijvende personen. Bovendien bestaan er noch voor betrokkenen uit de EU, noch voor betrokkenen uit de VS, mogelijkheden om toegang te krijgen tot gegevens of om deze te verbeteren of te wissen of om een administratief of gerechtelijk beroep in te stellen tegen het verzamelen en verder verwerken van hun persoonsgegevens in het kader van Amerikaanse observatieprogramma's.

---

[53] Zie bijlage I bij de veiligehavenbeschikking: "De naleving van de beginselen kan worden beperkt a) voor zover dit nodig is om aan de eisen van de nationale veiligheid, het algemeen belang en rechtshandhaving te voldoen; b) door wettelijke of bestuursrechtelijke bepalingen of rechtspraak die tegenstrijdige verplichtingen of uitdrukkelijke machtigingen scheppen, mits een organisatie die van een dergelijke machtiging gebruikmaakt, kan aantonen dat de niet-naleving van de beginselen beperkt is tot de mate die nodig is om de met de machtiging beoogde hogere legitieme belangen te waarborgen; of c) indien de richtlijn of de wetgeving van de betrokken lidstaat uitzonderingen of afwijkingen toestaat, mits deze ook in vergelijkbare contexten worden toegepast. In overeenstemming met het doel de bescherming van de persoonlijke levenssfeer te verbeteren, moeten organisaties ernaar streven deze beginselen volledig en op doorzichtige wijze toe te passen en in hun beleid inzake de bescherming van de persoonlijke levenssfeer aan te geven op welke gebieden er regelmatig op grond van punt b) uitzonderingen op de beginselen zullen worden toegestaan. Waar de beginselen en/of de wetgeving van de Verenigde Staten organisaties de mogelijkheid tot kiezen bieden, wordt daarom ook van hen verwacht dat zij waar mogelijk voor de hoogste mate van bescherming kiezen."

[54] Advies 4/2000 over het beschermingsniveau dat de veiligehavenbeginselen bieden, op 16 mei 2000 aangenomen door Groep gegevensbescherming artikel 29.

[55] Advies 4/2000 over het beschermingsniveau dat de veiligehavenbeginselen bieden, op 16 mei 2000 aangenomen door Groep gegevensbescherming artikel 29.

7.3. Transparantie

Ondernemingen geven niet systematisch in hun privacybeleid aan wanneer zij uitzonderingen op de beginselen toepassen. Burgers en ondernemingen zijn zich derhalve niet bewust van wat er met hun gegevens gebeurt. Dit is vooral van belang in verband met de werking van de betrokken Amerikaanse observatieprogramma's. Het gevolg is dat Europeanen wier gegevens in het kader van de veilige haven aan een onderneming in de VS worden doorgegeven, mogelijk niet door die onderneming op de hoogte worden gebracht van het feit dat hun gegevens toegankelijk kunnen worden gemaakt[56]. Dit doet de vraag rijzen of de veiligehavenbeginselen inzake transparantie worden nageleefd. Transparantie moet in de grootst mogelijke mate worden gegarandeerd zonder gevaar voor de nationale veiligheid. Naast bestaande vereisten voor ondernemingen om in hun privacybeleid aan te geven wanneer de beginselen kunnen worden beperkt door wettelijke of bestuursrechtelijke bepalingen of rechtspraak, zouden ondernemingen ook moeten worden aangemoedigd om in hun privacybeleid aan te geven wanneer zij de uitzonderingen op de beginselen toepassen om aan de eisen van de nationale veiligheid, het algemeen belang en rechtshandhaving te voldoen.

8. CONCLUSIES EN AANBEVELINGEN

Sinds de vaststelling ervan in 2000 is de veilige haven een middel geworden voor persoonsgegevensstromen tussen de EU en de VS. Het belang van een efficiënte bescherming in geval van doorgifte van persoonsgegevens is toegenomen ten gevolge van de enorme toename van de gegevensstromen die cruciaal zijn voor de digitale economie en de zeer belangrijke ontwikkelingen in het verzamelen, verwerken en gebruiken van gegevens. Internetondernemingen zoals Google, Facebook, Microsoft, Apple of Yahoo hebben honderden miljoenen klanten in Europa en geven persoonsgegevens voor verwerking door naar de VS op een schaal die in het jaar 2000, toen de veilige haven werd ingesteld, ondenkbaar was.

Als gevolg van een tekortkomingen op het gebeid van transparantie en handhaving van de regeling, blijven specifieke problemen bestaan en moeten deze worden aangepakt:

a) transparantie van het privacybeleid van veiligehavenleden,

b) doeltreffende toepassing van de privacybeginselen door ondernemingen in de VS, en

c) doeltreffendheid van de handhaving.

Bovendien doet de **grootschalige toegang van inlichtingendiensten tot gegevens die aan de VS zijn doorgegeven door in het kader van de veilige haven gecertificeerde ondernemingen**, nog meer serieuze vragen rijzen over de continuïteit van de gegevensbeschermingsrechten van Europeanen wanneer hun gegevens aan de VS worden doorgegeven.

Op basis van het bovenstaande formuleert de Commissie de volgende **aanbevelingen**:

Transparantie

1. *Ondernemingen met een zelfcertificering moeten hun privacybeleid publiek bekend maken.* Het volstaat niet dat ondernemingen het ministerie van Handel een

[56] Hierover wordt door sommige Europese ondernemingen die aan de veilige haven deelnemen, relatief transparante informatie gegeven. Nokia bijvoorbeeld, dat activiteiten in de VS uitoefent en aan de veilige haven deelneemt, voorziet in zijn privacybeleid in de volgende bepaling: *"We kunnen bij wet gedwongen worden om uw persoonlijke gegevens door te geven aan bepaalde autoriteiten of andere derden, bijvoorbeeld aan handhavingsinstanties in landen waar wij of derden namens ons actief zijn."*

beschrijving van hun privacybeleid geven. Het privacybeleid moet voor het publiek toegankelijk worden gemaakt op de websites van de ondernemingen, in duidelijke en ondubbelzinnige taal.

2. *Het privacybeleid op de websites van ondernemingen met een zelfcertificering zou steeds een link moeten bevatten naar de veiligehavenwebsite van het ministerie van Handel, waar alle "actuele" leden van de regeling worden vermeld*. Op die manier zullen de Europese betrokkenen onmiddellijk, zonder extra zoekopdrachten, kunnen verifiëren of een onderneming is aangesloten bij de veilige haven. Dit zou de geloofwaardigheid van de regeling helpen vergroten door de mogelijkheden voor ondernemingen te beperken om valselijk te beweren dat zij bij de veilige haven zijn aangesloten. In maart 2013 is het ministerie van Handel begonnen met ondernemingen daarom te verzoeken, maar dit proces zou moeten worden geïntensiveerd.

3. *Ondernemingen met een zelfcertificering zouden de privacyvoorwaarden van overeenkomsten die zij met subcontractanten sluiten, bijvoorbeeld voor cloudcomputing-diensten, moeten publiceren*. De veiligehavenregeling staat toe dat veiligehavenondernemingen met een zelfcertificering gegevens doorgeven aan derden die als hun "vertegenwoordigers" optreden, bijvoorbeeld aanbieders van clouddiensten. Wij menen te begrijpen dat in dergelijke gevallen het ministerie van Handel van de ondernemingen met een zelfcertificering verlangt dat zij een overeenkomst sluiten. Bij het sluiten van een dergelijke overeenkomst moet een veiligehavenonderneming echter ook het ministerie van Handel op de hoogte brengen en de privacywaarborgen publiek maken.

4. *Op de website van het ministerie van Handel moeten duidelijk alle ondernemingen worden aangeduid die geen actueel lid zijn van de regeling.* Het label "niet actueel" op de lijst van veiligehavenleden van het ministerie van Handel moet vergezeld gaan van een duidelijke waarschuwing dat een onderneming op dat ogenblik niet voldoet aan de veiligehavenvoorschriften. Ingeval de deelname "niet actueel" is, is de onderneming echter verplicht de veiligehavenvoorschriften te blijven toepassen op gegevens die zijn ontvangen in het kader van de veilige haven.

Verhaalsmogelijkheden

5. *Het privacybeleid op de websites van ondernemingen zou een link moeten bevatten naar de alternatieve geschillenbeslechter en/of het EU-panel.* Hierdoor zullen de Europese betrokkenen in geval van problemen onmiddellijk contact kunnen opnemen met de alternatieve geschillenbeslechter of het EU-panel. In maart 2013 is het ministerie van Handel begonnen met ondernemingen daarom te verzoeken, maar dit proces zou moeten worden geïntensiveerd.

6. *Alternatieve geschillenbeslechting moet direct beschikbaar en betaalbaar zijn.* Sommige instellingen voor alternatieve geschillenbeslechting in de veiligehavenregeling blijven burgers vergoedingen in rekening brengen — die zeer hoog kunnen zijn voor een individuele gebruiker — voor de behandeling van de klacht (200-250 dollar). In Europa daarentegen is toegang tot het gegevensbeschermingspanel voor het oplossen van klachten in het kader van de veiligehavenregeling kosteloos.

7. *Het ministerie van Handel zou meer systematisch aanbieders van alternatieve geschillenbeslechting moeten controleren met betrekking tot de transparantie en de toegankelijkheid van de informatie die zij verstrekken over de procedure die zij gebruiken en de follow-up die zij geven aan klachten.* Dit maakt geschillenbeslechting een doeltreffend en betrouwbaar mechanisme dat tot resultaten leidt. In dit verband moet er ook op worden gewezen dat de bekendmaking van geconstateerde gevallen van niet-naleving moet worden opgenomen in de reeks verplichte sancties van alternatieve geschillenbeslechters.

Handhaving

8. *Na de certificering of hercertificering van ondernemingen in het kader van de veilige haven, zou bij een bepaald percentage van deze ondernemingen ambtshalve moeten worden onderzocht of hun privacybeleid in overeenstemming is met de veiligehavenregeling (hetgeen verdergaat dan nagaan of aan de formele vereisten is voldaan).*

9. *Wanneer er sprake is van een geval van niet-naleving naar aanleiding van een klacht of een onderzoek, zou de betrokken onderneming na 1 jaar aan een specifiek follow-uponderzoek moeten worden onderworpen.*

10. *In geval van twijfel of een onderneming de veilige haven naleeft of over in behandeling zijnde klachten, moet het ministerie van Handel de bevoegde gegevensbeschermingsautoriteit uit de EU inlichten.*

11. *Het onderzoek naar valse aanspraken op deelname aan de veilige haven moet doorgaan.* Een onderneming die op zijn website beweert te voldoen aan de veiligehavenvoorschriften, maar die niet als "actueel" lid voorkomt op de lijst van het ministerie van Handel, misleidt consumenten en maakt misbruik van hun vertrouwen. Valse aanspraken tasten de geloofwaardigheid van het systeem als geheel aan en moeten daarom onmiddellijk van de websites van de ondernemingen worden verwijderd.

Toegang door de autoriteiten van de VS

12. *Het privacybeleid van ondernemingen met een zelfcertificering moet informatie bevatten over de mate waarin het recht van de VS toestaat dat overheidsinstanties gegevens die in het kader van de veilige haven zijn doorgegeven, verzamelen en verwerken. Met name moeten ondernemingen worden aangemoedigd om in hun privacybeleid aan te geven wanneer zij uitzonderingen op de beginselen toepassen om aan de eisen van de nationale veiligheid, het algemeen belang en rechtshandhaving te voldoen.*

13. *Het is belangrijk dat de uitzondering betreffende de nationale veiligheid waarin de veiligehavenbeschikking voorziet, uitsluitend wordt gebruikt in een mate die strikt noodzakelijk is en evenredig.*