BESCHIKKING 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

(Kennisgeving geschied onder nummer C(2000) 2441)

(Voor de EER relevante tekst)

(2000/520/EG)

DE COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap,

Gelet op 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], inzonderheid op artikel 25, lid 6,

Overwegende hetgeen volgt:

(1) Overeenkomstig 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 deze richtlijn al vóór de doorgifte wordt nageleefd.

(2) De Commissie kan vaststellen dat een derde land waarborgen voor een passend beschermingsniveau biedt. In dat geval kunnen persoonsgegevens zonder aanvullende garanties door de lidstaten worden doorgegeven.

(3) Overeenkomstig Richtlijn 95/46/EG dient het gegevensbeschermingsniveau te worden beoordeeld met inachtneming van alle omstandigheden waarin een gegevensdoorgifte of een categorie gegevensdoorgiften plaatsvindt en wordt in het bijzonder rekening gehouden met een aantal voorwaarden. De bij de richtlijn ingestelde Groep betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens [2] heeft richtsnoeren voor een dergelijke beoordeling vastgesteld [3].

(4) Gezien de verschillende benaderingen van gegevensbescherming in derde landen moeten de beoordeling van de gepastheid en besluiten op grond van artikel 25, lid 6, van Richtlijn 95/46/EG worden uitgevoerd op een wijze die geen willekeurige of onverantwoorde discriminatie tegen of tussen derde landen waar gelijksoortige voorwaarden gelden, noch een verkapte handelsbelemmering vormt, rekening houdend met de huidige internationale verbintenissen van de Gemeenschap.

(5) Het bij deze beschikking erkende passende beschermingsniveau voor de doorgifte van persoonsgegevens van de Gemeenschap naar de Verenigde Staten zou moeten worden bereikt indien organisaties voldoen aan de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer (Safe Harbor Privacy Principles), hierna „de beginselen" genoemd, en de richtsnoeren van de tenuitvoerlegging van de beginselen, de Vaak gestelde vragen (Frequently Asked Questions), hierna „FAQ's" genoemd, die op 21 juli 2000 door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd. Voorts zouden de organisaties hun beleid inzake de bescherming van de persoonlijke levenssfeer openbaar moeten maken en zich aan de rechtsbevoegdheid van de Federal Trade Commission (FTC) onderwerpen, overeenkomstig sectie 5 van de Federal Trade Commission Act waarin oneerlijke of misleidende handelingen of praktijken in of in verband met de handel worden verboden, dan wel aan die van een andere officiële instantie die de naleving van de overeenkomstig de FAQ's ten uitvoer gelegde beginselen daadwerkelijk garandeert.

(6) Sectoren en/of gegevensverwerking waarvoor niet een in bijlage VII van deze beschikking genoemde overheidsinstanties in de Verenigde Staten bevoegd is, dienen buiten het toepassingsgebied van deze beschikking te vallen.

(7) Voor een juiste toepassing van deze beschikking is het noodzakelijk dat de organisaties die de beginselen en de FAQ's onderschrijven, herkenbaar zijn voor de belanghebbende partijen, zoals de betrokkenen, degenen die gegevens naar het buitenland doorgeven en de gegevensbeschermingsautoriteiten. Hiertoe moet het ministerie van Handel van de Verenigde Staten of een door dit ministerie aangewezen instantie toezeggen een lijst bij te

[1] PB L 281 van 23.11.1995, blz. 31.

[2] Het internetadres van de groep is: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

[3] WP 12: Doorgifte van persoonsgegevens naar derde landen: toepassing van de artikelen 25 en 26 van de EU-richtlijn betreffende gegevensbescherming, goedgekeurd door de Groep op 24 juli 1998.

houden en ter beschikking te stellen van organisaties die door zelfcertificering de overeenkomstig de FAQ's ten uitvoer gelegde beginselen onderschrijven en die onder de rechtsbevoegdheid vallen van ten minste een van de in bijlage VII van deze beschikking genoemde overheidsinstanties.

(8) Ter wille van de doorzichtigheid en teneinde te garanderen dat de bevoegde autoriteiten in de lidstaten de personen wier persoonsgegevens worden verwerkt, kunnen beschermen, moet in deze beschikking worden aangegeven in welke buitengewone omstandigheden het gerechtvaardigd is specifieke gegevensstromen op te schorten, ook al is een passend beschermingsniveau vastgesteld.

(9) De door de beginselen en de FAQ's in het leven geroepen en door gevestigde mechanismen uit de overheids- en particuliere sector ondersteunde veilige haven vormt een innovatieve benadering, die eventueel moet worden herzien in het licht van de ervaring, de ontwikkelingen betreffende de bescherming van de persoonlijke levenssfeer in een situatie waarin de technologie de doorgifte en verwerking van persoonsgegevens steeds gemakkelijker maakt, en in het licht van rapporten van de betrokken met de rechtshandhaving belaste instanties over de uitvoering.

(10) De bij artikel 29 van de richtlijn opgerichte Groep betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens heeft over het beschermingsniveau dat door de Veiligehavenbeginselen in de Verenigde Staten wordt geboden, adviezen uitgebracht waarmee bij de voorbereiding van deze beschikking rekening is gehouden ([4]).

(11) De in deze beschikking vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 31 van Richtlijn 95/46/EG ingestelde comité,

([4]) WP 15: Advies 1/99 over het niveau van gegevensbescherming in de Verenigde Staten en het lopend overleg tussen de Europese Commissie en de regering van de Verenigde Staten.
WP 19: Advies 2/99 over het passend karakter van de „International Safe Harbor Principles" die op 19 april 1999 door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd.
WP 21: Advies 4/99 over de door het ministerie van Handel van de Verenigde Staten te publiceren Vaak gestelde vragen (FAQ's) met betrekking tot de voorgestelde Veiligehavenbeginselen.
WP 23: Werkdocument over de huidige stand van de lopende beraadslagingen tussen de Europese Commissie en de regering van de Verenigde Staten betreffende de „Internationale veiligehavenbeginselen".
WP 27: Advies 7/99 over het niveau van gegevensbescherming dat door de Veiligehavenbeginselen wordt geboden, die samen met de Vaak gestelde vragen (FAQ's) en andere documenten op 15 en 16 november 1999 door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd.
WP 31: Advies 3/2000 over de dialoog tussen de Europese Unie en de Verenigde Staten over de veiligehavenregeling.
WP 32: Advies 4/2000 over het beschermingsniveau van de Veiligehavenbeginselen.

HEEFT DE VOLGENDE BESCHIKKING GEGEVEN:

Artikel 1

1. Voor de toepassing van artikel 25, lid 2, van Richtlijn 95/46/EG geldt voor alle binnen de werkingssfeer van die richtlijn vallende activiteiten, dat de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer, hierna „de beginselen" genoemd, zoals vermeld in bijlage I van deze beschikking, ten uitvoer gelegd overeenkomstig de richtsnoeren in de Vaak gestelde vragen, hierna „FAQ's" genoemd, zoals vermeld in bijlage II van de beschikking, die op 21 juli 2000 door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd, worden geacht een passend beschermingsniveau te waarborgen voor de doorgifte van persoonsgegevens van de Gemeenschap naar in de Verenigde Staten gevestigde organisaties, een en ander gelet op de volgende, door het ministerie van Handel van de Verenigde Staten gepubliceerde documenten ten uitvoer gelegd volgens de ter uitvoering van die beginselen gegeven richtsnoeren:

a) een overzicht van de rechtshandhaving inzake de veilige haven, opgenomen in bijlage III;

b) een memorandum over schadevergoeding wegens inbreuken op de persoonlijke levenssfeer en uitdrukkelijke machtigingen in de wetgeving van de Verenigde Staten, opgenomen in bijlage IV;

c) een schrijven van de Federal Trade Commission, opgenomen in bijlage V;

d) een schrijven van het ministerie van Vervoer van de Verenigde Staten, opgenomen in bijlage VI.

2. Met betrekking tot elke doorgifte van gegevens moet aan de volgende voorwaarden zijn voldaan:

a) de organisatie die de gegevens ontvangt, heeft zich op eenduidige wijze en in het openbaar ertoe verbonden de beginselen die in overeenstemming met de FAQ's ten uitvoer worden gelegd, na te leven, en

b) de organisatie is onderworpen aan het wettelijk gezag van een in bijlage VII van deze beschikking vermelde overheidsinstantie in de Verenigde Staten die klachten kan onderzoeken en na oneerlijke en misleidende praktijken herstel kan verkrijgen alsmede schadeloosstelling voor natuurlijke personen, ongeacht het land van hun woonplaats of nationaliteit, indien de overeenkomstig de FAQ's ten uitvoer gelegde beginselen niet zijn nagekomen.

3. Elke organisatie die door zelfcertificering de overeenkomstig de FAQ's ten uitvoer gelegde beginselen onderschrijft, wordt geacht aan de in lid 2 gestelde voorwaarden te voldoen vanaf de datum waarop de organisatie het ministerie van Handel van de Verenigde Staten (of de door dit ministerie aangewezen instantie) in kennis stelt van de openbare bekendmaking van de in lid 2, onder a), bedoelde verbintenis, en van de identiteit van de in lid 2, onder b), bedoelde overheidsinstantie.

Artikel 2

Deze beschikking heeft alleen betrekking op de gepastheid van de bescherming die in de Verenigde Staten overeenkomstig de volgens de FAQ's ten uitvoer gelegde beginselen wordt geboden, teneinde aan de vereisten van artikel 25, lid 1, van Richtlijn 95/46/EG te voldoen en laat de toepassing van andere bepalingen van die richtlijn die op de verwerking van persoonsgegevens in de lidstaten betrekking hebben en met name van artikel 4, onverlet.

Artikel 3

1. Onverminderd hun bevoegdheden om maatregelen te nemen in verband met de naleving van nationale bepalingen die op grond van andere bepalingen dan artikel 25 van Richtlijn 95/46/EG zijn vastgesteld, kunnen de bevoegde autoriteiten in de lidstaten van hun bestaande bevoegdheden gebruikmaken om gegevensstromen naar een organisatie die door zelfcertificering de overeenkomstig de FAQ's ten uitvoer gelegde beginselen heeft onderschreven, op te schorten, teneinde personen ten aanzien van de verwerking van hun persoonsgegevens te beschermen, wanneer:

a) de in bijlage VII genoemde overheidsinstantie van de Verenigde Staten of een onafhankelijk verhaalmechanisme als bedoeld onder a) van het handhavingsbeginsel zoals vermeld in bijlage I van deze beschikking, tot de conclusie is gekomen dat de organisatie de overeenkomstig de FAQ's ten uitvoer gelegde beginselen schendt, of

b) het zeer waarschijnlijk is dat de beginselen 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 organisatie van het probleem in kennis te stellen en de gelegenheid te geven te reageren.

De opschorting wordt beëindigd zodra vaststaat dat de overeenkomstig de FAQ's ten uitvoer gelegde beginselen worden nageleefd en de bevoegde autoriteiten in de Gemeenschap hiervan in kennis zijn gesteld.

2. De lidstaten stellen de Commissie onverwijld in kennis wanneer op grond van lid 1 maatregelen worden genomen.

3. De lidstaten stellen de Commissie tevens in kennis van gevallen waarin instanties die voor de naleving van de overeenkomstig de FAQ's ten uitvoer gelegde beginselen in de Verenigde Staten verantwoordelijk zijn, verzuimen een dergelijke naleving te garanderen.

4. Wanneer uit de overeenkomstig de leden 1, 2 en 3 verzamelde informatie mocht blijken dat een instantie die verantwoordelijk is voor de naleving van de overeenkomstig de FAQ's ten uitvoer gelegde beginselen in de Verenigde Staten, haar taak niet naar behoren vervult, stelt de Commissie het ministerie van Handel van de Verenigde Staten hiervan in kennis en stelt zij zo nodig, in overeenstemming met de in artikel 31 van Richtlijn 95/46/EG vastgestelde procedure, ontwerpmaatregelen voor om deze beschikking in te trekken of op te schorten dan wel de werkingssfeer ervan te beperken.

Artikel 4

1. Deze beschikking kan te allen tijde worden aangepast in het licht van de bij de uitvoering ervan opgedane ervaringen en/of indien het door de beginselen en de FAQ's geboden beschermingsniveau door de in de wetgeving van de Verenigde Staten gestelde eisen wordt achterhaald.

In ieder geval evalueert de Commissie op basis van de beschikbare informatie de uitvoering van de beschikking drie jaar nadat de lidstaten ervan in kennis zijn gesteld, en deel zij alle relevante vaststellingen aan het bij artikel 31 van Richtlijn 95/46/EG ingestelde comité mee, inclusief alle gegevens die van invloed kunnen zijn op de overeenkomstig artikel 1 van deze beschikking gedane vaststelling dat het beschermingsniveau passend is in de zin van artikel 25 van Richtlijn 95/46/EG, alsmede alle gegevens waaruit blijkt dat deze beschikking op discriminerende wijze wordt uitgevoerd.

2. De Commissie legt zo nodig overeenkomstig de bij artikel 31 van Richtlijn 95/46/EG vastgestelde procedure een ontwerp van de te nemen maatregelen voor.

Artikel 5

De lidstaten nemen alle nodig maatregelen om uiterlijk negentig dagen na de kennisgeving ervan aan de lidstaten aan deze beschikking te voldoen.

Artikel 6

Deze beschikking is gericht tot de lidstaten.

Gedaan te Brussel, 26 juli 2000.

Voor de Commissie
Frederik BOLKESTEIN
Lid van de Commissie

BIJLAGE I

VEILIGEHAVENBEGINSELEN VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER

op 21 juli 2000 gepubliceerd door het ministerie van Handel van de Verenigde Staten

De wetgeving van de Europese Unie betreffende de bescherming van de persoonlijke levenssfeer, de gegevensbeschermingsrichtlijn („de richtlijn"), is op 25 oktober 1998 in werking getreden. Volgens deze richtlijn mogen persoonsgegevens alleen naar niet-EU-lidstaten worden doorgegeven als deze een „passend" beschermingsniveau van de persoonlijke levenssfeer bieden. De Verenigde Staten en de Europese Unie streven beide naar een betere bescherming van de persoonlijke levenssfeer van hun burgers, maar de Verenigde Staten hebben een andere benadering daarvan dan de Europese Unie. De aanpak van de Verenigde Staten is sectoraal en gebaseerd op een combinatie van wetgeving, regulering en zelfregulering. Gezien deze verschillen is bij veel organisaties in de Verenigde Staten onduidelijkheid ontstaan over de gevolgen van de door de Europese Unie geëiste „norm voor een passend beschermingsniveau" voor de doorgifte van persoonsgegevens uit de Europese Unie naar de Verenigde Staten.

Om deze onduidelijkheid te verminderen en een beter voorspelbaar kader voor deze gegevensdoorgifte te bieden publiceert het ministerie van Handel dit document en de Vaak gestelde vragen (FAQ's) („de beginselen") op grond van zijn wettelijke taak de internationale handel te bevorderen en te ontwikkelen. De beginselen zijn in samenspraak met het bedrijfsleven en het grote publiek opgesteld om de handel tussen de Verenigde Staten en de Europese Unie te vergemakkelijken. Ze zijn uitsluitend bedoeld om te worden gebruikt door organisaties in de Verenigde Staten die persoonsgegevens uit de Europese Unie ontvangen, om zo in aanmerking te komen voor de veilige haven en de hierdoor geboden veronderstelling van een „passend beschermingsniveau". Omdat de beginselen uitsluitend voor dit specifieke doel zijn ontworpen, kunnen ze voor andere doeleinden ongeschikt zijn. De beginselen kunnen de nationale bepalingen ter uitvoering van de richtlijn, die van toepassing zijn op de verwerking van persoonsgegevens in de lidstaten, niet vervangen.

Organisaties besluiten geheel vrijwillig of zij voor de veilige haven in aanmerking willen komen; zij kunnen dit op verschillende manieren doen. Organisaties die hiertoe besluiten, moeten de beginselen naleven om de voordelen van de veilige haven te krijgen en te behouden, en in het openbaar verklaren dat zij dit doen. Een organisatie die deelneemt aan een zelfreguleringsprogramma op het gebied van de bescherming van de persoonlijke levenssfeer dat de beginselen naleeft, komt er dan ook voor in aanmerking. Organisaties kunnen ook in aanmerking komen door een eigen zelfreguleringsbeleid terzake te ontwikkelen, dat zij met de beginselen in overeenstemming brengen. Indien een organisatie zich voor de naleving van de beginselen volledig of gedeeltelijk op zelfregulering baseert, maar de zelf vastgestelde regels niet naleeft, moet tegen haar vervolging kunnen worden ingesteld overeenkomstig sectie 5 van de Federal Trade Commission Act, die oneerlijke en misleidende handelingen verbiedt, dan wel ingevolge een andere wet of regeling die dergelijke praktijken verbiedt (zie de bijlage voor de lijst van door de Europese Unie erkende officiële instanties in de Verenigde Staten). Bovendien kunnen organisaties waarop wettelijke of bestuursrechtelijke bepalingen met betrekking tot een effectieve bescherming van persoonsgegevens van toepassing zijn, eveneens voor de voordelen van de veilige haven in aanmerking komen. De voordelen van de veilige haven gelden vanaf de datum dat de organisatie die hiervoor in aanmerking wil komen bij het ministerie van Handel (of een door dit ministerie aangewezen instantie) meldt dat zij de beginselen naleeft (zelfcertificering) overeenkomstig de richtsnoeren die in de Vaak gestelde vragen over zelfcertificering zijn uiteengezet.

De naleving van de beginselen kan worden beperkt a) voorzover 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.

Organisaties kunnen de beginselen om praktische of andere redenen op iedere verwerking van gegevens toepassen, maar zij zijn hiertoe alleen verplicht nadat zij tot de veilige haven zijn toegetreden. Om voor de veilige haven in aanmerking te komen zijn organisaties niet verplicht de beginselen toe te passen op persoonlijke informatie in handmatig bijgehouden gegevensbestanden. Organisaties die van de veilige haven gebruik willen maken om informatie in handmatig bijgehouden gegevensbestanden uit de Europese Unie te kunnen ontvangen, moeten de beginselen toepassen op alle informatie die wordt doorgegeven nadat zij tot de veilige haven zijn toegetreden. Als een organisatie wil dat personeelsgegevens bestaande uit persoonlijke informatie, die vanuit de Europese Unie in het kader van een arbeidsverhouding worden doorgegeven, eveneens onder de voordelen van de veilige haven vallen, moet zij dit in haar verklaring aan het ministerie van Handel (of de door dit ministerie aangewezen instantie) aangeven en voldoen aan de vereisten die zijn neergelegd in de FAQ over zelfcertificering. Organisaties kunnen de in artikel 26 van de richtlijn verlangde waar-

borgen ook bieden wanneer zij in contracten met organisaties die gegevens uit de Europese Unie doorgeven, de beginselen als belangrijke bepalingen over de bescherming van de persoonlijke levenssfeer opnemen, zodra de andere bepalingen voor dergelijke modelcontracten door de Commissie en de lidstaten zijn goedgekeurd.

De wetgeving van de Verenigde Staten is van toepassing op vragen betreffende de interpretatie en naleving van de Veiligehavenbeginselen (inclusief de Vaak gestelde vragen) en het desbetreffende beleid van veiligehavenorganisaties inzake de bescherming van de persoonlijke levenssfeer, behalve als deze organisaties zich ertoe verplicht hebben om met de Europese gegevensbeschermingsautoriteiten samen te werken. Tenzij anders vermeld zijn in voorkomend geval alle bepalingen van de Veiligehavenbeginselen en de Vaak gestelde vragen van toepassing.

Persoonsgegevens en persoonlijke informatie zijn gegevens over een specifieke of een identificeerbare persoon die onder het toepassingsgebied van de richtlijn vallen, vanuit de Europese Unie door een organisatie in de Verenigde Staten worden ontvangen en in de een of andere vorm zijn vastgelegd.

KENNISGEVING

Een organisatie moet particulieren in kennis stellen van de doeleinden waarvoor zij informatie over hen verzamelt en gebruikt, hoe particulieren voor vragen of klachten contact met de organisatie kunnen opnemen, aan welke derden de informatie bekend wordt gemaakt en welke keuzemogelijkheden en middelen de organisatie hen biedt om het gebruik en de bekendmaking van deze informatie te beperken. 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 bekendmaakt ([1]).

KEUZE

Een organisatie moet personen de mogelijkheid geven te kiezen of (zich ertegen te verzetten dat (opt-out)) hun persoonlijke informatie a) aan derden bekend zal worden gemaakt ([1]) of b) zal worden gebruikt voor een doel dat onverenigbaar is met 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 en betaalbare mechanismen worden geboden om deze keuze te maken.

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) moet de betrokkene positief of expliciet de mogelijkheid krijgen ervoor te kiezen (toestemming te geven (opt-in)) dat de informatie aan een derde bekend wordt gemaakt of zal worden gebruikt voor een ander doel dan waarvoor deze oorspronkelijk is verzameld of waarvoor de betrokkene achteraf zijn toestemming heeft gegeven. Een organisatie moet in ieder geval alle informatie die zij van een derde ontvangt en die deze derde als gevoelig aanmerkt en behandelt, als gevoelig behandelen.

VERDERE DOORGIFTE

Wanneer een organisatie informatie bekendmaakt aan een derde, moet zij het kennisgevings- en het keuzebeginsel toepassen. Wanneer zij informatie wil doorgeven aan een derde die als haar vertegenwoordiger optreedt, zoals in de eindnoot wordt beschreven, 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. Indien de organisatie aan deze eisen voldoet, zal zij niet aansprakelijk worden gehouden (tenzij door de organisatie anders wordt overeengekomen) indien een derde partij waaraan de informatie is doorgegeven, deze verwerkt op een manier die strijdig is met eventuele restricties of verklaringen, tenzij de organisatie wist of had moeten weten dat de derde partij de informatie op een dergelijke manier zou verwerken, maar geen redelijke maatregelen heeft genomen om deze verwerking te voorkomen of stop te zetten.

([1]) Er is geen kennisgeving nodig 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. Op een dergelijke bekendmaking is echter wel het beginsel van verdere doorgifte van toepassing.

BEVEILIGING

Organisaties die persoonlijke informatie verzamelen, bijhouden, gebruiken of verspreiden, moeten redelijke voorzorgsmaatregelen nemen om deze te beschermen tegen verlies, misbruik en ongeoorloofde toegang, bekendmaking, wijziging en vernietiging.

INTEGRITEIT VAN GEGEVENS

Overeenkomstig de beginselen moet persoonlijke informatie relevant zijn voor de doeleinden waarvoor deze zal worden gebruikt. 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. Voorzover dit voor deze doeleinden noodzakelijk is, moet een organisatie redelijke stappen ondernemen om ervoor te zorgen dat de gegevens betrouwbaar zijn voor het beoogde gebruik en dat ze correct, volledig en actueel zijn.

TOEGANG

Particulieren moeten toegang hebben tot de persoonlijke informatie die een organisatie over hen in bezit heeft, en deze informatie, voorzover deze onjuist is, kunnen corrigeren, wijzigen of verwijderen, tenzij de lasten of de kosten voor het verlenen van toegang niet in verhouding staan tot het gevaar voor de persoonlijke levenssfeer van de betrokkene, of tenzij de legitieme rechten van andere personen dan de betrokkene worden geschonden.

RECHTSHANDHAVING

Een doeltreffende bescherming van de persoonlijke levenssfeer moet ook mechanismen omvatten om de naleving van de beginselen te garanderen, alsmede verhaalmogelijkheden voor degenen op wie de gegevens betrekking hebben indien de beginselen niet worden nageleefd, en gevolgen voor een organisatie die zich niet aan de beginselen houdt. Deze mechanismen moeten ten minste het volgende omvatten: a) direct beschikbare en betaalbare onafhankelijke verhaalmechanismen voor het onderzoek en de afhandeling, aan de hand van de beginselen, van klachten en geschillen van particulieren en de toekenning van schadevergoedingen wanneer het toepasselijke recht of de initiatieven van de particuliere sector hierin voorzien; b) vervolgprocedures om na te gaan of de attesten en verklaringen van bedrijven over hun beleid inzake de bescherming van de persoonlijke levenssfeer waar zijn en of het voorgelegde beleid terzake ook ten uitvoer is gebracht zoals het is voorgesteld; en c) verplichtingen om problemen op te lossen die ontstaan doordat de beginselen niet worden nageleefd door organisaties die hebben verklaard deze na te leven en gevolgen voor dergelijke organisaties. De sancties moeten zwaar genoeg zijn om naleving door de organisaties te garanderen.

Bijlage

Lijst van door de Europese Unie erkende officiële instanties in de Verenigde Staten

De Europese Unie erkent de volgende overheidsinstanties in de Verenigde Staten als bevoegde instanties die klachten kunnen onderzoeken en na oneerlijke en misleidende praktijken herstel kunnen verkrijgen, alsmede schadeloosstelling voor de betrokkenen, indien de overeenkomstig de FAQ's ten uitvoer gelegde beginselen niet worden nagekomen:

— de Federal Trade Commission, krachtens haar bevoegdheid overeenkomstig sectie 5 van de Federal Trade Commission Act;

— het ministerie van Vervoer, krachtens zijn bevoegdheid overeenkomstig titel 49 van de United States Code, sectie 41712.

BIJLAGE II

VAAK GESTELDE VRAGEN (FAQ'S)

FAQ 1 — Gevoelige gegevens

V: *Moet een organisatie altijd toestemming geven voor de verwerking van gevoelige gegevens?*

A: Nee, toestemming is niet vereist wanneer de verwerking: 1. van vitaal belang is voor de betrokkene of voor iemand anders; 2. noodzakelijk is om rechtsvorderingen geldend te maken of om zich tegen een rechtsvordering te verweren; 3. noodzakelijk is voor het verstrekken van medische zorg of het stellen van een diagnose; 4. 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; 5. noodzakelijk is met het oog op de uitvoering van de arbeidsrechtelijke verplichtingen van de organisatie; of 6. betrekking heeft op gegevens waarvan duidelijk is dat ze door de betrokkene zelf openbaar zijn gemaakt.

FAQ 2 — Uitzonderingen voor journalistieke doeleinden

V: *Gelden, gezien de in de grondwet van de Verenigde Staten neergelegde bescherming van de persvrijheid en de in de richtlijn neergelegde vrijstelling voor journalistiek materiaal, de Veiligehavenbeginselen ook voor persoonlijke informatie die is verzameld, bewaard of verspreid voor journalistieke doeleinden?*

A: 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 van bescherming van de persoonlijke levenssfeer, moet 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. 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 Veiligehavenbeginselen.

FAQ 3 — Secundaire aansprakelijkheid

V: *Zijn aanbieders van internetdiensten, telecommunicatiebedrijven of andere organisaties uit hoofde van de Veiligehavenbeginselen aansprakelijk voor informatie die zij namens een andere organisatie enkel overbrengen, routeren, schakelen of opslaan, maar die wellicht in strijd is met hun voorwaarden?*

A: Nee. Evenmin als de richtlijn zelf voorziet de veilige haven in secundaire aansprakelijkheid. Wanneer een organisatie van een derde afkomstige informatie alleen doorgeeft, zonder de doeleinden en middelen van de verwerking van persoonlijke informatie vast te stellen, is zij niet aansprakelijk.

FAQ 4 — Investeringsbanken en accountants

V: *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 welke omstandigheden is dit volgens de beginselen van kennisgeving, keuze en toegang toelaatbaar?*

A: Investeringsbankiers en accountants mogen alleen informatie verwerken zonder dat de betrokkene hiervan op de hoogte is voorzover, 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 bedrijven 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.

FAQ 5 [1] **— De rol van de gegevensbeschermingsautoriteiten**

V: *Hoe zullen bedrijven die toezeggen met de gegevensbeschermingsautoriteiten uit de Europese Unie te zullen samenwerken, deze toezeggingen doen en hoe zullen deze gestand worden gedaan?*

A: In het kader van de veilige haven zijn organisaties uit de Verenigde Staten die persoonsgegevens uit de Europese Unie ontvangen, verplicht effectieve mechanismen aan te wenden om de naleving van de Veiligehavenbeginselen te waarborgen. Preciezer gezegd moeten zij, zoals vastgesteld in het rechtshandhavingsbeginsel, voorzien in a) verhaalmogelijkheden voor degenen op wie de gegevens betrekking hebben, b) vervolgprocedures om na te gaan of de attesten en verklaringen die zij over hun beleid inzake de bescherming van de persoonlijke levenssfeer hebben afgegeven, waar zijn, en c) verplichtingen om problemen op te lossen die ontstaan doordat organisaties de beginselen niet naleven, en consequenties hiervan voor dergelijke organisaties. Organisaties kunnen aan de punten a) en c) van het rechtshandhavingsbeginsel voldoen als zij zich houden aan te vereisten van deze FAQ voor de samenwerking met de gegevensbeschermingsautoriteiten.

Een organisatie kan zich ertoe verplichten met de gegevensbeschermingsautoriteiten samen te werken door in haar certificering voor de veilige haven bij het ministerie van Handel (zie FAQ 6 over zelfcertificering) te verklaren dat zij:

1. ervoor kiest aan de verplichtingen van de punten a) en c) van het rechtshandhavingsbeginsel van de veilige haven te voldoen door te beloven met de gegevensbeschermingsautoriteiten samen te werken;

2. met de gegevensbeschermingsautoriteiten zal samenwerken bij het onderzoek en de oplossing van klachten die in het kader van de veilige haven zijn ingediend; en

3. 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 Veiligehavenbeginselen 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.

De gegevensbeschermingsautoriteiten zullen op de volgende wijze hun medewerking verlenen door informatie en advies te geven:

— 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.

— Het panel zal aan de betrokken organisaties uit de Verenigde Staten advies verlenen over onopgeloste klachten van personen over de behandeling van persoonlijke informatie die vanuit de Europese Unie in het kader van de veilige haven is doorgegeven. Dit advies zal zo zijn opgesteld dat ervoor wordt gezorgd dat de Veiligehavenbeginselen correct worden toegepast en het zal de rechtsmiddelen noemen die volgens de gegevensbeschermingsautoriteiten de betrokkene(n) in aanmerking kan (kunnen) nemen.

— Het panel zal dit advies uitbrengen naar aanleiding van verwijzingen door de betrokken organisaties en/of rechtstreeks van personen ontvangen klachten tegen organisaties die zich ertoe verplicht hebben om in het kader van de Veiligehavenbeginselen 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.

— 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 dit 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.

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

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

[1] De opneming van deze FAQ in het pakket hangt af van de goedkeuring van de gegevensbeschermingsautoriteiten. Zij hebben de huidige tekst in de Groep van artikel 29 besproken en de meerderheid vindt deze aanvaardbaar, maar zij wensen slechts een definitief standpunt in te nemen in het kader van het algemene advies dat de Groep over het uiteindelijke pakket zal uitbrengen.

Organisaties die deze optie voor de oplossing van geschillen kiezen, moeten 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 of aan 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 (of de door dit ministerie aangewezen instantie) hiervan op de hoogte brengen zodat de lijst van veiligehavendeelnemers dienovereenkomstig kan worden gewijzigd. Elke niet-nakoming van de verplichting om met de gegevensbeschermingsautoriteiten samen te werken, alsmede elke niet-naleving van de Veiligehavenbeginselen kan op grond van sectie 5 van de FTC-wet of andere soortgelijke wetten als misleidende praktijk worden gevolgd.

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.

Gedurende een periode van drie jaar krijgen organisaties die tot de veilige haven toetreden de mogelijkheid om met de gegevensbeschermingsautoriteiten samen te werken. Voor afloop van deze periode zullen de gegevensbeschermingsautoriteiten deze regeling opnieuw bekijken als te veel organisaties uit de Verenigde Staten voor deze mogelijkheid kiezen.

FAQ 6 — Zelfcertificering

V: *Hoe kan een organisatie zelf een verklaring afleggen (zelfcertificering) dat zij de Veiligehavenbeginselen onderschrijft?*

A: De voordelen van de veilige haven zijn gegarandeerd vanaf de datum waarop een organisatie zelf aan het ministerie van Handel (of een door dit ministerie aangewezen instantie) verklaart de beginselen te onderschrijven (zelfcertificering). Hiervoor gelden de volgende richtsnoeren.

Voor zelfcertificering moet een organisatie die tot de veilige haven toetreedt een door een directielid ondertekende brief naar het ministerie van Handel (of de door dit ministerie aangewezen instantie) sturen, die ten minste de volgende informatie bevat:

1. naam van de organisatie, postadres, e-mailadres, telefoon- en faxnummer;
2. beschrijving van de activiteiten van de organisatie met betrekking tot de persoonlijke informatie die zij uit de Europese Unie ontvangt; en
3. beschrijving van het beleid van de organisatie inzake de bescherming van de persoonlijke levenssfeer ten aanzien van dergelijke persoonlijke informatie, waaronder:
   a) waar dit door het publiek kan worden geraadpleegd,
   b) de datum van inwerkingtreding,
   c) 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 de veilige haven,
   d) 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 bescherming van de persoonlijke levenssfeer te behandelen (en die wordt vermeld in de bijlage van de beginselen),
   e) de naam van programma's ter bescherming van waaraan de organisatie deelneemt,
   f) de wijze van controle (bv. intern, door derden) [2], en
   g) het onafhankelijke verhaalmechanisme dat onopgeloste klachten kan onderzoeken.

Als een organisatie wil dat personeelsgegevens die vanuit de Europese Unie in het kader van een arbeidsverhouding zijn doorgegeven, eveneens onder de voordelen van de veilige haven vallen, kan zij dit doen indien er een officiële instantie is die bevoegd is tot de behandeling van tegen de organisatie ingebrachte klachten in verband met de in de bijlage van de beginselen vermelde personeelsgegevens. Bovendien moet zij dit in haar brief aangeven en verklaren zich ertoe te verplichten dat ze, waar FAQ 9 en FAQ 5 van toepassing zijn, in overeenstemming met deze FAQ's met de betrokken EU-autoriteit(en) zal samenwerken en dat ze het advies van deze autoriteiten zal naleven.

Het ministerie (of de door het ministerie aangewezen instantie) zal een lijst bijhouden van alle organisaties die dergelijke brieven indienen, en zo in het genot komen van de voordelen van de veilige haven, en de lijst bijwerken

[2] Zie FAQ 7 over controle.

aan de hand van de jaarlijkse brieven en kennisgevingen die het ingevolge FAQ 11 ontvangt. Deze zelfcertificeringsbrieven moeten minstens eens per jaar worden ingediend. Anders wordt de organisatie van de lijst verwijderd en zijn de voordelen van de veilige haven niet langer gegarandeerd. Zowel de lijst als de door de organisaties ingediende verklaringen zullen voor het publiek toegankelijk worden gemaakt. Alle organisaties die zelf een verklaring met betrekking tot de veilige haven afleggen, moeten in de verklaringen die zij publiceren over hun beleid inzake de bescherming van de persoonlijke levenssfeer ook aangeven dat zij de Veiligehavenbeginselen onderschrijven.

Voor gegevens die worden ontvangen tijdens de periode waarin de organisatie de voordelen van de veilige haven geniet, is de verplichting de beginselen na te leven niet in de tijd beperkt; deze blijven op die gegevens van toepassing zolang de organisatie ze opslaat, gebruikt of openbaar maakt, zelfs indien de organisatie de veilige haven nadien om enigerlei reden verlaat.

Een organisatie die ten gevolge van een fusie of overname haar rechtspersoonlijkheid als zelfstandige onderneming zal verliezen, moet het ministerie van Handel (of een door dit ministerie aangewezen instantie) hiervan vooraf in kennis stellen. In deze kennisgeving moet ook worden vermeld of de overnemende onderneming of de onderneming die door de fusie ontstaat 1. onder de wetgeving die op de overname of fusie van toepassing is, nog steeds verplicht is zich aan de Veiligehavenbeginselen te houden of 2. verkiest de Veiligehavenbeginselen zelf te onderschrijven of andere garanties biedt, zoals een schriftelijke verklaring dat zij de Veiligehavenbeginselen zal naleven. Als noch 1 noch 2 van toepassing is, moeten alle gegevens die in het kader van de veilige haven zijn verkregen, onmiddellijk worden verwijderd.

Een organisatie hoeft de Veiligehavenbeginselen niet op alle persoonlijke informatie toe te passen, maar moet deze vanaf het moment van toetreding tot de veilige haven wel toepassen op alle uit de Europese Unie ontvangen persoonlijke informatie.

De Federal Trade Commission of een andere bevoegde overheidsinstantie kan actie ondernemen tegen iedere onjuiste verklaring aan het grote publiek met betrekking tot de naleving van de Veiligehavenbeginselen door een organisatie. Bij onjuiste verklaringen tegenover het ministerie van Handel (of de door dit ministerie aangewezen instantie) kan vervolging worden ingesteld op grond van de False Statements Act (18 U.S.C. § 1001).

FAQ 7 — Controle

V: *Hoe voorzien organisaties in vervolgprocedures om na te gaan of de attesten en verklaringen die zij over hun beleid inzake de bescherming van de persoonlijke levenssfeer in het kader van de veilige haven afleggen, waar zijn en of dit beleid is uitgevoerd zoals het is voorgesteld en of het beantwoordt aan de Veiligehavenbeginselen?*

A: Teneinde aan de controle-eisen van het rechtshandhavingsbeginsel te voldoen kan een organisatie de naleving van dergelijke attesten en verklaringen nagaan door zelfbeoordeling of door externe nalevingscontroles.

Bij de zelfbeoordelingsmethode moet uit de controle blijken dat het beleid van een organisatie inzake de bescherming van de persoonlijke levenssfeer bij 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 Veiligehavenbeginselen, 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 in de uitvoering van het beleid en dat er disciplinaire maatregelen tegen hen worden genomen indien zij dit niet doen, 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.

Organisaties moeten hun informatiebestanden over de tenuitvoerlegging van hun beleid inzake de bescherming van de persoonlijke levenssfeer in het kader van de veilige haven 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 de instantie die oneerlijke en misleidende praktijken moet onderzoeken.

Indien de organisatie voor een externe controle van de naleving heeft gekozen, moet hieruit blijken dat het beleid inzake de bescherming van de persoonlijke levenssfeer met betrekking tot uit de Europese Unie ontvangen persoonlijke informatie in overeenstemming is met de Veiligehavenbeginselen, 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.

FAQ 8 — Toegang

Toegangsbeginsel

Particulieren moeten toegang heben tot de persoonlijke informatie die een organisatie over hen in bezit heeft, en deze informatie, voorzover deze onjuist is, kunnen corrigeren, wijzigen of verwijderen, tenzij de lasten of de kosten voor het verlenen van toegang niet in verhouding staan tot het gevaar voor de persoonlijke levenssfeer van de betrokkene, of tenzij de legitieme rechten van andere personen dan de betrokkene worden geschonden.

V1: *Is het recht op toegang absoluut?*

A: Nee. Volgens de Veiligehavenbeginselen is het recht op toegang fundamenteel voor de bescherming van de persoonlijke levenssfeer. Met name geeft dit recht de betrokkene de mogelijkheid om de juistheid van de informatie die over hem wordt bijgehouden, na te gaan. Toch is op de verplichting die een organisatie heeft om toegang te verlenen tot de informatie die zij over een persoon in haar bezit heeft, het beginsel van evenredigheid of redelijkheid van toepassing en moet die verplichting daarom in sommige gevallen worden afgezwakt. De toelichting bij de richtsnoeren van de OESO inzake de bescherming van de persoonlijke levenssfeer uit 1980 toont duidelijk aan dat de verplichting tot toegangverlening voor een organisatie niet absoluut is. De verplichting betekent niet dat er een buitengewoon grondig onderzoek kan worden verricht zoals dat bijvoorbeeld het geval is bij een dagvaarding noch dat toegang moet worden verleend tot alle verschillende vormen waarin de informatie door de organisatie kan worden bewaard.

Uit ervaring is gebleken dat organisaties zich bij een verzoek van een particulier om toegang om te beginnen zouden moeten 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 wordt verlangd. De organisatie kan bijvoorbeeld nagaan met welke afdeling(en) van de organisatie de betrokkene contact heeft gehad en/of voor welk soort informatie (of het gebruik ervan) toegang wordt gevraagd. Particulieren behoeven een verzoek om toegang tot hun eigen gegevens echter niet te motiveren.

Kosten en lasten zijn belangrijke factoren die in overweging moeten worden genomen, maar zij kunnen niet de doorslag geven bij een beslissing over de redelijkheid van toegang. Indien de 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 FAQ's, deze informatie ter beschikking stellen, ook al is dit vrij moeilijk of duur.

Indien de gevraagde informatie niet gevoelig is of niet wordt gebruikt voor beslissingen die voor de betrokkene van groot belang zijn (bv. niet-gevoelige marketinggegevens die worden gebruikt om te beslissen of al dan niet een catalogus naar de betrokkene wordt gestuurd), maar meteen beschikbaar is en zonder dat het veel kost kan worden gegeven, dan moet de organisatie toegang verlenen tot de feitelijke informatie die zij over de betrokkene bewaart. Deze informatie kan feiten omvatten die van de betrokkene zelf zijn verkregen, feiten die tijdens een transactie zijn verzameld of feiten over de betrokkene die van anderen afkomstig zijn.

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 informatie waarvoor toegang is gevraagd, moet de organisatie de beschermde informatie bewerken en de andere beschikbaar stellen. Indien een organisatie besluit dat de toegang in een bepaald geval moet worden ontzegd, dient zij de betrokkene uit te leggen waarom zij tot dit besluit is gekomen en een contactadres op te geven waar de betrokkene met vragen terecht kan.

V2: *Wat is vertrouwelijke commerciële informatie en kunnen organisaties iemand de toegang ontzeggen om het vertrouwelijke karakter van de informatie te beschermen?*

A: Vertrouwelijke commerciële informatie („confidential commercial information", een term die in de Federal Rules of Civil Procedure gebruikt wordt ten aanzien van de inzage van stukken) is informatie die een organisatie tegen openbaarmaking beschermt, wanneer openbaarmaking concurrenten zou helpen. Het computerprogramma dat een organisatie gebruikt (bv. voor het opstellen van modellen) of de details van dat programma kunnen vertrou-

welijke commerciële informatie zijn. Wanneer het mogelijk is vertrouwelijke commerciële informatie probleemloos te scheiden van andere informatie waarvoor toegang is gevraagd, moet de organisatie de vertrouwelijke commerciële informatie bewerken en de niet-vertrouwelijke informatie beschikbaar stellen. Organisaties kunnen iemand de toegang tot de informatie ontzeggen dan wel de toegang beperken wanneer anders hun eigen vertrouwelijke commerciële informatie (volgens bovenstaande definitie), zoals door de organisatie opgestelde marketingconclusies en classificaties, aan de dag zou komen, of de vertrouwelijke commerciële informatie van een andere organisatie voorzover op deze informatie een contractuele geheimhoudingverplichting van toepassing is in situaties waarin een dergelijke geheimhoudingsverplichting normaal wordt aangegaan of opgelegd.

V3: *Betekent het verlenen van toegang dat een organisatie aan de betrokkenen hun persoonlijke informatie uit haar gegevensbanken ter beschikking moet stellen of moet de organisatie de betrokkenen toegang tot de gegevensbank zelf verlenen?*

A: Toegang verlenen betekent dat de organisatie de betrokkenen de informatie ter beschikking moet stellen, niet dat hen toegang tot de gegevensbank van de organisatie zelf moet worden verleend.

V4: *Moet een organisatie haar gegevensbanken zodanig herstructureren dat zij toegang kan verlenen?*

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

V5: *Uit deze antwoorden blijkt dat in sommige omstandigheden de toegang kan worden ontzegd. Onder welke andere omstandigheden kan een organisatie particulieren de toegang tot hun persoonlijke informatie ontzeggen?*

A: Dergelijke omstandigheden zijn beperkt en er moeten concrete redenen zijn om iemand de toegang te ontzeggen, bijvoorbeeld wanneer belangrijke openbare belangen, zoals de defensie of de nationale of openbare veiligheid, 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:

a) belemmering van de uitvoering of de handhaving van de wet, inclusief het voorkomen, onderzoeken of opsporen van misdrijven, of van het recht op een eerlijk proces;

b) belemmering van civielrechtelijke procedures, inclusief het voorkomen of onderzoeken van rechtsvorderingen en opsporingen dienaangaande, of van het recht op een eerlijk proces;

c) openbaarmaking van persoonlijke informatie over derden, die niet kan worden bewerkt;

d) schending van beroepsrechten of -plichten die al dan niet voortvloeien uit de wet;

e) schending van de noodzakelijke geheimhouding van toekomstige of lopende onderhandelingen, bijvoorbeeld over de aankoop van beursgenoteerde ondernemingen;

f) conflict met veiligheidsonderzoeken of klachtenprocedures waarbij werknemers zijn betrokken;

g) aantasting van de geheimhouding die in een bepaalde periode noodzakelijk kan zijn in verband met personeelsbeleid en bedrijfsherstructurering;

h) aantasting van de geheimhouding die noodzakelijk kan zijn voor toezichthoudende of regulerende taken in verband met een gezond economisch of financieel beheer; of

i) andere omstandigheden waarin de lasten of de kosten van het verlenen van toegang in geen verhouding staan tot de hiermee behaalde voordelen of wanneer de gerechtvaardigde rechten en belangen van anderen worden geschaad.

Een organisatie die zich op een uitzondering beroept, moet aantonen dat die uitzondering van toepassing is (zoals normaal het geval is). Zoals hierboven reeds is gezegd, moeten de redenen voor het weigeren of beperken van de toegang aan de betrokkenen worden medegedeeld en moet hun een contactadres worden opgegeven waar zij met verdere vragen terecht kunnen.

V6: *Kan een organisatie kosten in rekening brengen voor het verlenen van toegang?*

A: Ja. In de richtsnoeren van de OESO wordt dit recht erkend, op voorwaarde dat het tarief niet te hoog is. Organisaties mogen dus voor het verlenen van toegang een redelijk tarief vragen. Dit kan trouwens nuttig zijn om herhaaldelijke en lastige verzoeken tegen te gaan.

Organisaties die openbaar beschikbare informatie verkopen, kunnen dus 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.

De toegang kan niet op kostengronden worden geweigerd als de betrokkene bereid is deze kosten te betalen.

V7: *Moet een organisatie toegang verlenen tot persoonlijke informatie die uit openbare bestanden komt?*

A: Ter verduidelijking, openbare bestanden zijn bestanden die door overheidsdiensten op alle mogelijke niveaus worden bewaard en die voor iedereen toegankelijk zijn. Het is niet nodig het toegangsbeginsel op deze informatie toe te passen, voorzover deze niet wordt gecombineerd met andere persoonlijke informatie, tenzij het hierbij gaat om kleine stukjes informatie uit niet-openbare bestanden 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 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, voorzover niet andere toegestane uitzonderingen op deze informatie van toepassing zijn.

V8: *Moet het toegangsbeginsel worden toegepast op openbaar beschikbare persoonlijke informatie?*

A: Net als voor informatie uit openbare bestanden (zie V 7) is het niet nodig toegang te verlenen tot informatie die reeds voor iedereen beschikbaar is, voorzover deze niet wordt gecombineerd met niet-openbaar beschikbare informatie.

V9: *Hoe kan een organisatie zich tegen herhaaldelijke of lastige verzoeken om toegang beschermen?*

A: Een organisatie hoeft op dergelijke verzoeken niet in te gaan. Organisaties kunnen daartoe een redelijk tarief in rekening brengen en 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 zoals de frequentie waarmee de informatie wordt bijgewerkt, het doel waarvoor de gegevens worden gebruikt en de aard van de informatie.

V10: *Hoe kan een organisatie zich beschermen tegen frauduleuze verzoeken om toegang?*

A: 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.

V11: *Is er een termijn waarbinnen een organisatie op verzoeken om toegang moet reageren?*

A: Ja, organisaties moeten zonder buitensporige vertraging en binnen een redelijke termijn antwoord geven. Aan deze eis kan op verschillende manieren worden voldaan, zoals in de toelichting bij de richtsnoeren inzake de bescherming van de persoonlijke levenssfeer van de OESO uit 1980 is beschreven. De voor de verwerking verantwoordelijke die op regelmatige tijdstippen informatie aan de betrokkenen verstrekt, kan worden vrijgesteld van de verplichting meteen op elk verzoek te reageren.

FAQ 9 — Personeel

V1: *Valt de overdracht van persoonlijke informatie die in het kader van een arbeidsverhouding is verzameld, van de Europese Unie naar de Verenigde Staten onder de veilige haven?*

A: Ja, wanneer een EU-bedrijf persoonlijke informatie over zijn (voormalige of huidige) werknemers, die het in het kader van een arbeidsverhouding heeft verzameld, doorgeeft aan een moederbedrijf, dochterbedrijf of een niet-geaffilieerde dienstverlener in de Verenigde Staten die aan de veilige haven deelneemt, zijn de Veiligehavenbeginselen

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 op de doorgifte die deze wetgeving stelt, in acht moeten worden genomen.

De Veiligehavenbeginselen zijn alleen van toepassing wanneer bestanden over individueel bepaalde personen worden doorgegeven of toegankelijk worden gemaakt. Statistische informatie die berust op geaggregeerde personeelsgegevens en/of gegevens die zijn geanonimiseerd of waarbij gebruik is gemaakt van pseudoniemen, geven geen aanleiding tot problemen in verband met de bescherming van de persoonlijke levenssfeer.

V2: *Hoe zijn de kennisgevings- en keuzebeginselen op dergelijke informatie van toepassing?*

A: Een organisatie in de Verenigde Staten die in het kader van de veilige haven personeelsgegevens uit de Europese Unie heeft ontvangen, mag deze informatie alleen in overeenstemming met het kennisgevings- en het keuzebeginsel aan derden bekend maken en/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 keuze laten, tenzij dezen al toestemming hadden gegeven om de informatie voor dergelijke doeleinden te gebruiken. Bovendien mag hun keuze niet van invloed zijn op de carrièremogelijkheden van de werknemers noch mag deze straf tot gevolg hebben.

Voor sommige 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.

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

Voorzover en zolang het noodzakelijk is de legitieme belangen van een organisatie te beschermen in verband met bevorderingen, benoemingen of andere besluiten ten aanzien van de werknemers, hoeft een organisatie het kennis- en het keuzebeginsel niet toe te passen.

V3: *Hoe wordt het toegangsbeginsel toegepast?*

A: De FAQ's over toegang verschaffen 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 Veiligehavenbeginselen moet een organisatie die dergelijke gegevens in de Verenigde Staten verwerkt, deze toegang direct of via de werkgever in de Europese Unie verlenen.

V4: *Hoe werkt de rechtshandhaving voor personeelsgegevens in het kader van de Veiligehavenbeginselen?*

A: Voorzover informatie alleen in het kader van een arbeidsverhouding wordt gebruikt, ligt de primaire verantwoordelijkheid voor de gegevens ten opzichte van de werknemer bij de onderneming in de Europese Unie. Hieruit volgt dat Europese werknemers die over schending 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 nationale gegevensbeschermingsautoriteit of arbeidsrechtbank. Dit geldt ook voor gevallen waarin het beweerde misbruik van de persoonlijke informatie in de Verenigde Staten heeft plaatsgehad en onder de verantwoordelijkheid valt van de organisatie uit de Verenigde Staten die de informatie van de werkgever heeft ontvangen, en niet onder die van de werkgever zelf. In dergelijke gevallen gaat het dus om een schending van de Veiligehavenbeginselen en niet van de nationale wetgeving tot uitvoering van de richtlijn. 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 ter bescherming van de persoonlijke levenssfeer.

Een aan de veilige haven deelnemende organisatie in de Verenigde Staten die gebruikmaakt van in het kader van een arbeidsverhouding vanuit de Europese Unie doorgegeven gegevens over het personeel in de Europese Unie en die wil dat dergelijke doorgiften onder de veilige haven 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. De gegevensbeschermingsautoriteiten die met een dergelijke samenwerking instemmen, moeten de Europese Commissie en het ministerie van Handel hiervan in kennis stellen. Als een organisatie uit de Verenigde Staten die aan de veilige haven deelneemt, personeelsgegevens wil doorgeven vanuit een lidstaat waarvan de gegevensbeschermingsautoriteit niet met dergelijke doorgiften instemt, zijn de bepalingen van FAQ 5 van toepassing.

FAQ 10 — Artikel 17 — contracten

V: *Is er een contract vereist wanneer gegevens alleen om ze te laten verwerken uit de Europese Unie naar de Verenigde Staten worden doorgegeven, ongeacht het feit of de verwerker al dan niet aan de veilige haven deelneemt?*

A: Ja. De voor de verwerking verantwoordelijken in Europa moeten altijd een contract sluiten wanneer gegevens alleen voor verwerking worden doorgegeven, ongeacht of dit binnen de Europese Unie of daarbuiten gebeurt. De bedoeling van een contract is de bescherming van de belangen van de voor de verwerking verantwoordelijke, d.w.z. de persoon of de instantie die het doel van en de middelen voor de gegevensverwerking vaststelt en die jegens de betrokkene(n) de volle verantwoordelijkheid voor de gegevens draagt. In het contract worden dus behalve de uit te voeren verwerking de maatregelen gespecificeerd die noodzakelijk zijn om te garanderen dat de gegevens veilig zijn.

Een organisatie in de Verenigde Staten die aan de veilige haven deelneemt en persoonlijke informatie uit Europa alleen voor verwerking ontvangt, behoeft derhalve niet de beginselen op deze informatie toe te passen, omdat overeenkomstig de desbetreffende EU-regeling (die strenger kan zijn dan de overeenkomstige Veiligehavenbeginselen) de voor de gegevens verantwoordelijke in de Europese Unie hiervoor tegenover de betrokkene verantwoordelijk blijft.

Aangezien door de veiligehavendeelnemers passende bescherming wordt verleend, is er voor contracten met veiligehavendeelnemers, die alleen de verwerking van gegevens ten doel hebben, geen voorafgaande toestemming nodig (of deze toestemming wordt automatisch door de lidstaten verleend), hetgeen voor contracten met ontvangers die niet aan de veilige haven deelnemen of die geen passende bescherming bieden, wel vereist is.

FAQ 11 — Afhandeling van geschillen en rechtshandhaving

V: *Hoe moet aan de in het rechtshandhavingsbeginsel gestelde eisen inzake de afhandeling van geschillen worden voldaan en hoe zal een organisatie in geval van permanente niet-naleving van de beginselen worden aangepakt?*

A: Het rechtshandhavingsbeginsel stelt de eisen vast waaraan handhaving van de Veiligehavenbeginselen moet voldoen. Hoe aan de eisen van punt b) van het beginsel moet worden voldaan, wordt in FAQ 7 (Controle) uiteengezet. Deze FAQ 11 handelt over de punten a) en c), die beide onafhankelijke verhaalmechanismen vereisen. Deze mechanismen kunnen verschillende vormen hebben, maar moeten aan de eisen van het rechtshandhavingsbeginsel voldoen. Organisaties kunnen op de volgende wijze aan deze eisen voldoen: 1. door naleving van programma's van de particuliere sector inzake de bescherming van de persoonlijke levenssfeer, die de Veiligehavenbeginselen in hun voorschriften integreren en doeltreffende handhavingsmechanismen omvatten zoals die welke in het rechtshandhavingsbeginsel worden beschreven; 2. door zich te onderwerpen aan wettelijke of regulerende toezichthoudende autoriteiten die individuele klachten behandelen en geschillen afhandelen; of 3. door zich ertoe te verbinden met de gegevensbeschermingsautoriteiten in de Europese Gemeenschap of hun gemachtigde vertegenwoordigers samen te werken. Deze lijst is bedoeld ter illustratie en is niet uitputtend. De particuliere sector kan andere handhavingsmechanismen ontwikkelen mits deze aan de eisen van het rechtshandhavingsbeginsel en van de FAQ's voldoen. Er zij op gewezen dat de eisen van het rechtshandhavingsbeginsel een aanvulling zijn op de eis die is geformuleerd in de derde alinea van de inleiding op de beginselen, namelijk dat bepalingen die het resultaat zijn van zelfregulering moeten kunnen worden gehandhaafd op grond van sectie 5 van de Federal Trade Commission Act of een soortgelijke wet.

Verhaalmechanismen

De consumenten moeten worden aangemoedigd eventuele klachten met de desbetreffende organisatie te bespreken alvorens een beroep te doen op onafhankelijke verhaalmechanismen. De onafhankelijkheid van een verhaalmechanisme kan op verschillende wijzen worden aangetoond, bijvoorbeeld door een transparante samenstelling en financiering of door de gebleken ervaring. Zoals in het rechtshandhavingsbeginsel wordt geëist, moet het verhaalmechanisme voor particulieren direct beschikbaar en betaalbaar 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 Veiligehavenbeginselen toegepaste praktijken inzake de bescherming van de persoonlijke levenssfeer ([3]). Zij moeten ook meewerken bij de ontwikkeling van hulpmiddelen als gestandaardiseerde klachtenformulieren om de klachtenafhandelingsprocedure te vergemakkelijken.

Rechtsmiddelen en sancties

De rechtsmiddelen die de geschillenafhandelingsinstantie biedt, moeten ertoe leiden dat de gevolgen van de niet-naleving door de organisatie, voorzover 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 ([4]). 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 geschillenafhandelingsinstanties en zelfregulerende instanties moeten in voorkomend geval de rechter of de terzake bevoegde overheidsinstantie in kennis stellen van de niet-inachtneming van hun uitspraken door veiligehavenorganisaties, en het ministerie van Handel (of de door dit ministerie aangewezen instantie) daarvan op de hoogte stellen.

Actie van de FTC

De FTC zal prioriteit geven aan zaken die haar door zelfregulerende organisaties voor de bescherming van de persoonlijke levenssfeer, zoals BBBOnline en TRUSTe, en de lidstaten van de Europese Unie in verband met niet-naleving van de Veiligehavenbeginselen worden voorgelegd, om na te gaan of er sprake is van schending van sectie 5 van de FTC Act, die oneerlijke of bedrieglijke handelspraktijken verbiedt. Als de FTC reden(en) heeft om aan te nemen dat sectie 5 werd geschonden, kan zij de zaak oplossen door een administratief verbod van de aangeklaagde praktijken te laten uitvaardigen, of door bij een federale rechtbank een klacht in te dienen, die als deze wordt aanvaard, kan resulteren in een uitspraak die hetzelfde effect sorteert. 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 Handel van dergelijke acties in kennis stellen. Dit ministerie moedigt andere overheidsinstanties ertoe aan hem van het uiteindelijke resultaat van dergelijke verwijzingen of andere uitspraken in verband met de naleving van de Veiligehavenbeginselen in kennis te stellen.

Permanente niet-naleving

Als een organisatie voortdurend de beginselen overtreedt, komt ze niet langer in aanmerking voor de voordelen van de veilige haven. Er is sprake van permanente niet-naleving indien een organisatie die bij het ministerie van Handel (of de door dit ministerie aangewezen instantie) een zelfcertificeringsverklaring heeft ingediend, weigert zich te conformeren aan een definitieve uitspraak van een zelfregulerende of 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 van Handel (of de door dit ministerie aangewezen instantie) daarvan dan onverwijld in kennis stellen. Als zij dit niet doet, kan op grond van de False Statements Act vervolging tegen deze organisatie worden ingesteld.

Indien het ministerie (of de door dit ministerie aangewezen instantie) ervan in kennis wordt gesteld dat een organisatie de beginselen voortdurend overtreedt, ongeacht of deze kennisgeving uitgaat van de organisatie zelf, van een zelfregulerende instantie of van een overheidsinstantie, zal het dit vermelden op de openbare lijst van organisaties die zelf hebben verklaard de veilige haven in acht te zullen nemen, evenwel met dien verstande dat het de organisatie die de beginselen niet heeft nageleefd, daarvan 30 dagen van tevoren in kennis heeft gesteld en de kans heeft gegeven om te reageren. Uit deze door het ministerie van Handel (of de door dit ministerie aangewezen instantie) bijgehouden openbare lijst blijkt dan ook welke organisaties verder voor de voordelen van de veilige haven in aanmerking komen en welke niet.

([3]) Geschillenafhandelingsinstanties hoeven het rechtshandhavingsbeginsel niet in acht te nemen. Zij kunnen ook van de beginselen afwijken in geval van strijdige verplichtingen of een uitdrukkelijke machtiging bij de uitvoering van hun specifieke taken.

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

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

FAQ 12 — Keuze — Tijdstip van verzet (opt-out)

V: *Houdt het keuzebeginsel in dat een persoon zijn keuzerecht alleen aan het begin van een relatie kan uitoefenen of kan hij dit te allen tijde?*

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 direct 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, bevorderen. In ieder geval moet de betrokkene een beroep kunnen doen op een direct beschikbaar en betaalbaar mechanisme om dit keuzerecht uit te oefenen.

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.

FAQ 13 — Reisinformatie

V: *Wanneer mag 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, aan organisaties buiten de Europese Unie worden doorgegeven?*

A: Dergelijke informatie mag onder verschillende omstandigheden 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 1. dit noodzakelijk is om de door de passagier gevraagde diensten te leveren of voor de uitvoering van de vervoersovereenkomst, zoals een bonusregeling; of 2. de passagier op ondubbelzinnige wijze met de doorgifte heeft ingestemd. Organisaties in de Verenigde Staten die aan de veilige haven 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 de veilige haven 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 de veilige haven 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.

FAQ 14 — Farmaceutische en medische producten

V1: *Zijn op persoonsgegevens die in de Europese Unie zijn verzameld en voor farmaceutisch onderzoek en/of voor andere doeleinden naar de Verenigde Staten zijn doorgegeven, de wetten van de lidstaten of de Veiligehavenbeginselen van toepassing?*

A: De wetgeving van de lidstaten is van toepassing op de verzameling van de persoonsgegevens, alsmede op de verwerking voorzover die plaatsvindt vóór de doorgifte aan de Verenigde Staten. De Veiligehavenbeginselen 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.

V2: *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 veiligehavendeelnemer in de Verenigde Staten, mag deze de gegevens dan gebruiken voor nieuw wetenschappelijk onderzoek?*

A: Ja, mits de betrokkene hiervan in eerste instantie op de juiste wijze van 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. 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 gegevens oorspronkelijk zijn verzameld of waarvoor het individu later toestemming heeft gegeven, is opnieuw toestemming vereist.

V3: *Wat gebeurt er met de gegevens van een deelnemer aan een klinische proef die zelf of op verzoek van de opdrachtgever zijn medewerking aan de proef opzegt?*

A: Deelnemers kunnen op ieder moment hun medewerking aan een klinische proef opzeggen, of hiertoe worden verzocht. Alle gegevens 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.

V4: *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. Is een soortgelijke doorgifte ook toegestaan aan anderen, zoals ondernemingen en andere onderzoekers?*

A: Ja, mits dit in overeenstemming is met de beginselen van kennisgeving en keuze.

V5: *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. Kunnen de deelnemers aan zulke klinische proeven (aangeduid als „blinde" tests) tijdens de proef toegang krijgen tot de gegevens over hun behandeling?*

A: Nee, de deelnemer hoeft geen toegang tot deze gegevens te krijgen 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. 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 hij in het kader van de medische proef is behandeld en in tweede instantie tot de opdrachtgever van de proef.

V6: *Moeten producenten van geneesmiddelen en medische apparatuur de Veiligehavenbeginselen met betrekking tot kennisgeving, keuze, verdere doorgifte en toegang in acht nemen 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 (bv. een pacemaker) gebruiken?*

A: Nee, voorzover 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.

V7: *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. Is een doorgifte van dusdanig gecodeerde gegevens van de Europese Unie naar de Verenigde Staten een doorgifte van persoonsgegevens waarop de Veiligehavenbeginselen van toepassing zijn?*

A: Nee. Dit geldt niet als een doorgifte van persoonsgegevens waarop de beginselen van toepassing zijn.

FAQ 15 — Informatie uit openbare bestanden of openbaar beschikbare informatie

V: *Moeten de beginselen van kennisgeving, keuze en verdere doorgifte worden toegepast op informatie uit openbare bestanden of openbaar beschikbare informatie?*

A: Het is niet nodig de beginselen van kennisgeving, keuze en 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 en 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.

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 de veilige haven in aanmerking.

BIJLAGE III

Veilige haven: overzicht rechtshandhaving

Bevoegdheden van de centrale overheid en de staten op het gebied van oneerlijke en misleidende praktijken en de bescherming van de persoonlijke levenssfeer

In dit memorandum wordt een beeld gegeven van de bevoegdheden van de Federal Trade Commission (FTC) in het kader van sectie 5 van de Federal Trade Commission Act (15 U.S.C. §§ 41-58, zoals gewijzigd) om maatregelen te nemen tegen organisaties die persoonlijke informatie niet beschermen, ondanks hun verklaringen en/of verplichtingen dat wel te doen. Ook wordt aandacht besteed aan de uitzonderingen op deze bevoegdheden en aan andere instanties van de centrale overheid of de staten die maatregelen kunnen nemen wanneer de FTC daartoe niet bevoegd is [1].

De bevoegdheid van de FTC bij oneerlijke en misleidende praktijken

Volgens sectie 5 van de Federal Trade Commission Act zijn „oneerlijke of misleidende handelingen of praktijken in of in verband met de handel" illegaal. 15 U.S.C. § 45(a)(1). Sectie 5 verleent de FTC volmacht om dergelijke handelingen en praktijken te voorkomen. 15 U.S.C. § 45(a)(2). De FTC kan na een formele behandeling van de zaak het laakbare gedrag verbieden. 15 U.S.C. § 45(b). In het openbaar belang kan de FTC eventueel ook bij een districtsrechtbank vragen om een tijdelijke beperking of een tijdelijk of permanent verbod. 15 U.S.C. § 53(b). In gevallen waarin de oneerlijke of misleidende handelingen of praktijken wijdverbreid zijn, of wanneer zij terzake al een verbod heeft uitgevaardigd, kan zij een administratieve beslissing afkondigen om dergelijke handelingen of praktijken in het algemeen te verbieden. 15 U.S.C. § 57a.

Niet-naleving van een voorschrift van de FTC kan bestraft worden met een civielrechtelijke boete van maximaal 11 000 USD, waarbij iedere dag dat de overtreding voortduurt een afzonderlijke overtreding vormt [2], 15 U.S.C. § 45(1). Ook degene die bewust een beslissing van de FTC overtreedt, kan voor iedere overtreding worden bestraft met een boete van 11 000 USD. 15 U.S.C § 45(m). Handhaving kan worden afgedwongen door het ministerie van Justitie of, indien dit weigert, de FTC. 15 U.S.C. § 56.

De bevoegdheden van de FTC op het gebied van de bescherming van de persoonlijke levenssfeer

Wanneer de FTC haar bevoegdheden uit hoofde van sectie 5 uitoefent, neemt zij het standpunt in dat een onjuiste verklaring over de reden waarom informatie bij klanten wordt verzameld of hoe de informatie zal worden gebruikt een misleidende praktijk is [3]. Zo heeft de FTC in 1998 een klacht tegen GeoCities ingediend omdat dit bedrijf, ondanks verklaringen van het tegendeel, informatie die het op zijn website had verzameld aan derden bekendmaakte, zodat dezen de consument zonder diens voorafgaande toestemming met reclame konden bestoken [4]. FTC-medewerkers hebben ook verklaard dat het verzamelen van persoonlijke informatie bij kinderen en de verkoop en bekendmaking van deze informatie zonder de toestemming van de ouders waarschijnlijk een oneerlijke praktijk is [5].

---

[1] We gaan hier niet in op alle federale wetten waarin de bescherming van de persoonlijke levenssfeer in een specifieke context aan de orde komt of op de wetten van de staten en het ongeschreven recht die van toepassing zijn. Tot de federale wetgeving waarin de verzameling en het gebruik van persoonlijke informatie voor commerciële doeleinden worden geregeld, behoren onder meer de Cable Communications Policy Act (47 U.S.C. § 551), de Driver's Privacy Protection Act (18 U.S.C. § 2721), de Electronic Communications Privacy Act (18 U.S.C. § 2701 e.v.), de Electronic Funds Transfer Act (15 U.S.C. §§ 1693, 1693m), de Fair Credit Reporting Act (15 U.S.C. § 1681 e.v.), de Right to Financial Privacy Act (12 U.S.C. § 3401 e.v.), de Telephone Consumer Protection Act (47 U.S.C. § 227) en de Video Privacy Protection Act (18 U.S.C. § 2710). In vele staten bestaat op deze gebieden soortgelijke wetgeving, zie bv. Mass. Gen Laws ch. 167B, § 16 (waarbij het financiële instellingen wordt verboden financiële gegevens over een klant aan derden bekend te maken zonder dat deze toestemming heeft gegeven en zonder wettelijke procedure), N. Y. Pub. Health Law § 17 (beperking van het gebruik en de bekendmaking van medische of psychiatrische gegevens en toegang tot deze gegevens voor patiënten).

[2] In een dergelijke zaak kan de districtsrechtbank ook maatregelen opleggen waarmee naleving van het FTC-voorschrift kan worden afgedwongen. 15 U.S.C. § 45(1).

[3] „Misleidende praktijk" wordt gedefinieerd als een verklaring, een omissie of een handeling die waarschijnlijk tot gevolg heeft dat verstandige consumenten op belangrijke punten worden misleid.

[4] Zie www.ftc.gov/opa/1998/9808/geocitie.htm.

[5] Zie de brief aan Center for Media Education, www.ftc.gov/os/1997/9707/cenmed.htm. Bovendien verleent de Children's Online Privacy Protection Act van 1998 de FTC een specifieke wettelijke bevoegdheid om de verzameling van persoonlijke informatie bij kinderen via websites en door exploitanten van on-linediensten te reguleren. Zie 15 U.S.C. §§ 6501-6506. In het bijzonder verlangt deze wet van de exploitanten dat zij hun voornemen bekendmaken en dat zij controleerbare toestemming van de ouders krijgen voordat ze persoonlijke informatie bij kinderen verzamelen, en deze gebruiken of bekendmaken. Id., § 6502(b). De ouders krijgen in de wet ook een recht van toegang, alsmede het recht om toestemming voor een voortgezet gebruik van de informatie te weigeren. Id.

De voorzitter van de FTC, Robert Pitofsky, wees er in zijn brief van 23 september 1998 aan de heer John Mogg, directeur-generaal bij de Europese Commissie, op dat de bevoegdheid van de FTC om de persoonlijke levenssfeer te beschermen beperkt is wanneer er geen onjuiste verklaring (of in het geheel geen verklaring) is gegeven over de wijze waarop de verzamelde informatie zal worden gebruikt. Bedrijven die van de voorgestelde veilige haven willen profiteren, zullen evenwel moeten verklaren dat zij de door hen verzamelde informatie overeenkomstig de voorgeschreven richtsnoeren zullen beschermen. Wanneer een bedrijf verklaart dat het de privacy van de informatie zal waarborgen en dat vervolgens niet doet, is er dan ook sprake van een onjuiste verklaring en een „misleidende praktijk" in de zin van sectie 5.

Aangezien de bevoegdheden van de FTC alleen betrekking hebben op oneerlijke of misleidende handelingen of praktijken „in of in verband met de handel", is zij niet bevoegd ten aanzien van de verzameling en het gebruik van persoonlijke informatie voor niet-commerciële doeleinden, zoals de inzameling van fondsen voor charitatieve doeleinden. Zie brief Pitofsky, blz. 3. Anders is het gesteld bij het gebruik van persoonlijke informatie bij commerciële transacties. Wanneer een werkgever bijvoorbeeld persoonlijke informatie over zijn werknemers aan een direct-marketingbedrijf verkoopt, valt deze transactie wel onder sectie 5.

Uitzonderingen op sectie 5

Sectie 5 noemt uitzonderingen op de bevoegdheden van de FTC over oneerlijke of misleidende handelingen of praktijken met betrekking tot:

— financiële instellingen (banken, spaarbanken, kredietinstellingen);

— telecommunicatiebedrijven en algemene binnenlandsvervoerbedrijven;

— luchtvaartmaatschappijen; en

— de vee- en vleeshandel.

Zie 15 U.S.C, § 45(a)(2). Hieronder bespreken we iedere uitzondering, met de regulerende autoriteit die in de plaats van de FTC treedt.

Financiële instellingen ([6])

De eerste uitzondering heeft betrekking op „banken en spaarbanken zoals gedefinieerd in sectie 18(f)(3) [15 U.S.C. § 57a(f)(3)]" en „federale kredietinstellingen zoals gedefinieerd in sectie 18(f)(4) [15 U.S.C. § 57a(f)(4)]" ([7]). Deze financiële instellingen vallen in plaats daarvan onder regelingen van respectivelijk de Federal Reserve Board, het Office of Thrift Supervision ([8]) en de National Credit Union Administration Board. Zie 15 U.S.C. § 57a(f). Deze regulerende instanties moeten voorschriften geven die nodig zijn om oneerlijke of misleidende praktijken van deze financiële instellingen te voorkomen ([9]) en moeten een afzonderlijke afdeling oprichten voor de behandeling van klachten van consumenten. 15 U.S.C. § 57a(f)(1). Ten slotte vloeien bevoegdheden op het gebied van de rechtshandhaving voort uit sectie 8 van de Federal Deposit Insurance Act (12 U.S.C. § 1818) voor banken en spaarbanken en uit de secties 120 en 206 van de Federal Credit Union Act voor federale kredietinstellingen. 15 U.S.C. §§ 57a(f)(2)-(4).

Hoewel het verzekeringswezen in de lijst van uitzonderingen in sectie 5 niet specifiek wordt genoemd, laat de McCarran-Ferguson Act (15 U.S.C. § 1011 e.v.) de regulering van het verzekeringswezen in het algemeen over aan de afzon-

([6]) Op 12 november 1999 heeft President Clinton de Gramm-Leach-Bliley Act ondertekend (Pub. L. 106-102, gecodificeerd in 15 U.S.C. § 6801 e.v.). De wet beperkt de bekendmaking door financiële instellingen van persoonlijke informatie over hun klanten en verlangt van hen onder meer dat ze al hun klanten in kennis stellen van hun privacybeleid en praktijken ten aanzien van het verstrekken van persoonlijke informatie aan geaffilieerde en niet-geaffilieerde bedrijven. De wet machtigt de FTC, de federale bankautoriteiten en andere autoriteiten regelingen vast te stellen om de door de wet vereiste bescherming van de persoonlijke levenssfeer ten uitvoer te leggen. Deze instanties hebben de hiertoe voorgestelde regelingen uitgevaardigd.

([7]) Terminologisch gezien is deze uitzondering niet van toepassing op de aandelensector. Makelaars, handelaars en andere in de effectenhandel werkzame personen vallen, voor wat hun oneerlijke of misleidende handelingen en praktijken betreft, dus zowel onder de jurisdictie vande Securities and Exchange Commission als onder die van de FTC.

([8]) De uitzondering in sectie 5 had oorspronkelijk betrekking op de Federal Home Loan Bank Board, die in augustus 1989 in het kader van de Financial Institutions Reform, Recovery and Enforcement Act werd afgeschaft. De functies ervan werden overgenomen door het Office of Thrift Supervision, de Resolution Trust Corporation, de Federal Deposit Insurance Corporation en de Housing Finance Board.

([9]) Hoewel financiële instellingen niet langer onder de bevoegdheid van de FTC vallen, bepaalt sectie 5 ook dat wanneer de FTC een regel over oneerlijke of misleidende handelingen of praktijken uitvaardigt, de Financial Regulatory Boards binnen 60 dagen soortgelijke voorschriften moeten goedkeuren. Zie 15 U.S.C. § 57a(f)(1).

derlijke staten ([10]). Ingevolge sectie 2(b) van de McCarran-Ferguson Act kan federaal recht een regulering van een staat niet buiten werking stellen, hieraan geen afbreuk doen, noch in de plaats van een dergelijke regeling treden „tenzij die federale wet specifiek betrekking heeft op het verzekeringswezen". 15 U.S.C. § 1012(b). De bepalingen van de FTC Act hebben evenwel betrekking op het verzekeringswezen „voorzover dit niet in de wet van een staat is geregeld". Id. De McCarran-Ferguson Act voegt zich alleen naar de wetgeving van de staten met betrekking tot „het verzekeringswezen". De FTC behoudt dus nog bevoegdheden over oneerlijke of misleidende praktijken van verzekeringsmaatschappijen wanneer dit niet op het verzekeringswezen betrekking heeft. Dit is bijvoorbeeld het geval wanneer verzekeraars persoonlijke informatie over hun polishouders verkopen aan direct-marketingbedrijven voor andere dan verzekeringsproducten ([11]).

Algemene vervoerbedrijven

De tweede uitzondering van sectie 5 betreft algemene vervoerbedrijven waarop de wetgeving ter regulering van de handel van toepassing is. 15 U.S.C. § 45(a)(2). In dit geval gaat het hierbij om subtitel IV van titel 49 van de United States Code en om de Communications Act van 1934 (47 U.S.C. § 151 e.v.) (de Communications Act). Zie 15 U.S.C. § 44.

49 U.S.C. subtitel IV (Interstate Transportation) heeft betrekking op het vervoer per spoor, over de weg en over water en op makelaars, expeditiebedrijven en exploitanten van pijpleidingen. 49 U.S.C. § 10101 e.v. Al deze algemene vervoerbedrijven worden gereguleerd door de Surface Transportation Board, een onafhankelijk agentschap binnen het ministerie van Vervoer. 49 U.S.C. §§ 10501, 13501 en 15301. In ieder geval mag het vervoerbedrijf geen informatie openbaar maken over de aard, de bestemming en andere aspecten van zijn vracht, die ten koste van de verzender zou kunnen worden gebruikt. Zie 49 U.S.C. §§ 11904, 14908 en 16103. Deze bepalingen hebben betrekking op informatie over de vracht en dus niet over persoonlijke informatie over de verzender die geen verband houdt met de vracht.

In de Communications Act wordt bepaald dat de nationale en internationale handel in draadgebonden en draadloze communicatie wordt geregeld door de Federal Communications Commission (FCC). Zie 47 U.S.C. §§ 151 en 152. De Communications Act heeft niet alleen betrekking op algemene telecommunicatiemaatschappijen, maar ook op radio-, televisie- en kabelbedrijven die niet algemeen zijn en als zodanig niet in aanmerking komen voor de uitzondering van sectie 5 van de FTC Act. De FTC is derhalve bevoegd onderzoek te doen naar oneerlijke en misleidende praktijken van deze maatschappijen, terwijl de FCC tegelijkertijd zijn eigen onafhankelijke bevoegdheden terzake kan uitoefenen.

Krachtens de Communications Act is iedere telecommunicatiemaatschappij, waaronder ook lokale telefooncentrales, verplicht informatie over hun klanten vertrouwelijk te behandelen ([12]). 47 U.S.C. § 222(a). Afgezien van deze algemene bevoegdheden ter bescherming van de persoonlijke levenssfeer werd de Communications Act gewijzigd bij de Cable Communications Policy Act van 1984 (de Cable Act), 47 U.S.C. § 521 e.v., om kabelexploitanten te verplichten tot een vertrouwelijke behandeling van „persoonlijk identificeerbare informatie" over kabelabonnees. 47 U.S.C. § 551 ([13]). De Cable Act beperkt het verzamelen van persoonlijke informatie door kabelexploitanten en verplicht hen hun abonnees in kennis te stellen van de aard van de verzamelde informatie en van de wijze waarop deze wordt gebruikt. De Cable Act geeft de abonnees recht op toegang tot informatie over zichzelf en eist van de kabelexploitanten dat deze informatie die niet langer nodig is, vernietigt.

De Communications Act machtigt de FCC deze twee privacybepalingen te handhaven, hetzij op eigen initiatief, hetzij naar aanleiding van een klacht ([14]). 47 U.S.C. §§ 205, 403; id. § 208. Indien de FCC vaststelt dat een telecommunicatiemaatschappij (of een kabelexploitant) de privacybepalingen van sectie 222 of sectie 551 heeft geschonden, heeft zij in wezen de keus uit drie mogelijke acties. In de eerste plaats kan de FCC, na de partijen te hebben gehoord en de overtre-

([10]) „Het verzekeringswezen en iedere hierbij betrokken persoon is onderworpen aan de wetten van de staten, die betrekking hebben op de regulering of de belastingheffing van de betrokken bedrijven." 15 U.S.C. § 1012(a).

([11]) De FTC heeft in verschillende contexten jurisdictie gehad over verzekeringsinstellingen. In een geval nam zij maatregelen tegen een bedrijf dat misleidende advertenties plaatste in een staat waar het geen bedrijfsvergunning had. De FTC was bevoegd omdat de regulering van de staat niet van toepassing was daar het bedrijf zich in werkelijkheid buiten de jurisdictie van de staat bevond. Zie FTC v. Travelers Health Association, 362 U.S. 293 (1960).
Zeventien staten hebben het door de National Association of Insurance Commissioners (NAIC) opgestelde model voor een „Insurance Information and Privacy Protection Act" goedgekeurd. Deze wet bevat bepalingen over kennisgeving, gebruik, bekendmaking en toegang. Bijna alle staten hebben ook het model van de NAIC voor een „Unfair Insurance Practices Act" goedgekeurd, die specifiek gericht is op oneerlijke handelspraktijken in het vezekeringswezen.

([12]) De term „netwerkinformatie over klanten" heeft betrekking op informatie over de „hoeveelheid, technische configuratie, type, bestemming en mate van gebruik van een telecommunicatiedienst" door een klant en informatie over zijn telefoonrekening. 47 U.S.C. § 222(f)(1). De term heeft evenwel niet betrekking op informatie over abonnementen. Id.

([13]) De wetgeving geeft geen expliciete definitie van „persoonlijk identificeerbare informatie".

([14]) Deze bevoegdheid omvat het recht op herstel bij overtredingen van de bescherming van de persoonlijke levenssfeer in het kader van sectie 222 van de Communications Act of, ten aanzien van kabelabonnees, sectie 551 van de door de Cable Act aangebrachte wijziging op de wet. Zie ook 47 U.S.C. § 551(f)(3) (een civielrechtelijke actie in een federale districtsrechtbank is een niet-exclusief rechtsmiddel dat de kabelabonnee ten dienste staat in aanvulling op ieder ander rechtsmiddel dat de wet hem biedt).

ding te hebben vastgesteld, de maatschappij verplichten tot een schadevergoeding ([15]). 47 U.S.C. § 209. Zij kan de maatschappij echter ook opdragen op te houden met de laakbare praktijken of omissies. 47 U.S.C. § 205(a). Ten slotte kan de Commissie de betrokken maatschappij ertoe verplichten iedere regeling of praktijk die de FCC mocht voorschrijven in acht te nemen en na te leven. Id.

Particulieren die van mening zijn dat een telecommunicatiemaatschappij of kabelexploitant de desbetreffende bepalingen van de Communications Act of de Cable Act heeft overtreden, kunnen een klacht bij de FCC indienen of een zaak direct aan een federale districtsrechtbank voorleggen. 47 U.S.C. § 207. Een klager die in een zaak tegen een telecommunciatiemaatschappij over het niet-beschermen van informatie over klanten in het kader van de ruimere sectie 222 van de Communications Act van een federaal gerecht gelijk krijgt, kan een schadevergoeding krijgen en ook kunnen zijn advocaatkosten worden vergoed. 47 U.S.C. § 206. Een klager die in het kader van de speciaal op kabelexploitanten van toepassing zijnde sectie 551 van de Cable Act wegens een vermeende inbreuk op de privacy een rechtsvordering indient, kan behalve een vergoeding van de feitelijke schade en van zijn advocaatkosten ook nog een als straf bedoelde schadevergoeding en een redelijke vergoeding van zijn procedurekosten krijgen. 47 U.S.C. § 551(f).

De FCC heeft gedetailleerde regels ter uitvoering van sectie 222 vastgesteld. Zie 47 CFR 64.2001-2009. Deze bevatten specifieke waarborgen ter bescherming van netwerkinformatie over klanten tegen ongeoorloofde toegang. De voorschriften verlangen van telecommunicatiebedrijven dat ze:

— softwaresystemen ontwikkelen en gebruiken waarin de kennisgevings-/goedkeuringsstatus van een klant wordt aangegeven wanneer het dossier van de klant voor het eerst op het scherm komt;

— een elektronisch „controlespoor” aanhouden om na te gaan wie wanneer en waarom toegang heeft gehad tot het dossier van de klant;

— hun medewerkers opleiden in het geautoriseerde gebruik van netwerkinformatie over klanten en bruikbare disciplinaire maatregelen vaststellen;

— procedures instellen om bij externe marketing op de naleving toe te zien; en

— de FCC jaarlijks in kennis stellen van de wijze waarop zij deze regels naleven.

Luchtvaartmaatschappijen

Sectie 5 van de FTC Act is evenmin van toepassing op Amerikaanse en buitenlandse luchtvaartmaatschappijen waarop de Federal Aviation Act van 1958 van toepassing is. Zie 15 U.S.C. § 45(a)(2). Dit omvat ieder bedrijf dat nationaal of internationaal goederen- of reizigersvervoer of postvervoer door de lucht aanbiedt. Zi 49 U.S.C. § 40102. Voor luchtvaartmaatschappijen is het ministerie van Vervoer bevoegd. De minister van Vervoer kan actie ondernemen ter voorkoming van oneerlijke, misleidende, uitbuiting veroorzakende of concurrentiebelemmerende praktijken in het luchtvervoer. 49 U.S.C. § 40101(a)(9). Wanneer dit in het openbaar belang is, kan hij ook nagaan of een Amerikaanse of buitenlandse luchtvaartmaatschappij of een reisbureau oneerlijke of misleidende praktijken uitvoert. 49 U.S.C. § 41712. Na de partijen te hebben gehoord kan de minister van Vervoer bevelen de illegale praktijk stop te zetten. Id. Voorzover onze kennis reikt, is deze bevoegdheid nooit uitgeoefend in het kader van de bescherming van persoonlijke informatie over luchtvaartreizigers ([16]).

Twee bepalingen ter bescherming van persoonlijke informatie zijn in specifieke contexten op luchtvaartmaatschappijen van toepassing. Ten eerste beschermt de Federal Aviation Act de persoonlijke levenssfeer van degenen die als piloot solliciteren. Zie 49 U.S.C. § 44936(f). Weliswaar mogen luchtvaartmaatschappijen een dossier over het arbeidsleven van de sollicitant aanleggen, maar de wet geeft de sollicitant het recht te weten dat een dossier is opgevraagd, toestemming te geven voor het verzoek, onnauwkeurigheden te corrigeren en te verlangen dat het dossier alleen wordt bekendgemaakt aan degenen die bij zijn aanwerving betrokken zijn. Ten tweede verlangen de voorschriften van het ministerie van Vervoer dat informatie over de passagierslijst die ten behoeve van de overheid wordt verzameld voor gebruik in geval van een vliegramp, geheim wordt gehouden en alleen wordt bekendgemaakt aan het ministerie van Buitenlandse Zaken, de National Transportation Board (op verzoek van de National Transportation Safety Board) en het ministerie van Vervoer. 14 CFR part 243, § 243.9(c) (zoals toegevoegd bij 63 FR 8258).

([15]) De afwezigheid van directe schade voor de klager is evenwel geen reden om de klacht af te wijzen. 47 U.S.C. § 208(a).

([16]) Er schijnen binnen de bedrijfstak pogingen gaande te zijn om de privacykwestie te behandelen. Vertegenwoordigers van de bedrijfstak hebben de voorgestelde Veiligehavenbeginselen en de mogelijke toepassing ervan op luchtvaartmaatschappijen besproken. Ook is er gesproken over een voorstel voor een beleid ter bescherming van de persoonlijke levenssfeer voor de bedrijfstak waarbij de deelnemende ondernemingen zich uitdrukkelijk onderwerpen aan de bevoegdheden van het ministerie van Vervoer.

Vee- en vleeshandel

Volgens de Packers and Stockyards Act van 1921 (7 U.S.C. § 181, e.v.) is het handelaren in vee, vlees, vleeswaren, niet-industrieel bewerkte producten van vee, alsmede pluimveehandelaren met betrekking tot levend pluimvee verboden oneerlijke, onterecht discriminerende of misleidende praktijken of middelen te gebruiken of zich hiermee in te laten. 7 U.S.C. § 192(a); zie ook 7 U.S.C. § 213(a) (waarin oneerlijke, onterecht discriminerende of misleidende praktijken of middelen met betrekking tot vee verboden zijn). De minister van Landbouw is als eerste verantwoordelijk voor de handhaving van deze bepalingen, terwijl de FTC bevoegd is voor detailhandeltransacties en transacties met betrekking tot de pluimvee-industrie. 7 U.S.C. § 227(b)(2).

Het is niet duidelijk of de minister van Landbouw het feit dat een vee- of vleeshandelaar de persoonlijke levenssfeer niet in overeenstemming met zijn verklaringen dienaangaande beschermt als een misleidende praktijk in de zin van de Packers and Stockyards Act zal beschouwen. De uitzondering van sectie 5 is evenwel alleen dan op particulieren, partnerschappen of vennootschappen van toepassing wanneer op hen de Packers and Stockyards Act van toepassing is. Indien de bescherming van de persoonlijke levenssfeer in het kader van de Packers and Stockyards Act geen thema is, is de uitzondering van sectie 5 wellicht niet van toepassing en zijn vee- en vleeshandelaren in dat opzicht onderworpen aan de bevoegdheden van de FTC.

Bevoegdheid van de staten bij oneerlijke en misleidende praktijken

Volgens een analyse van FTC-medewerkers beschikken alle 50 staten plus het District of Columbia, Guam, Puerto Rico en de Amerikaanse Maagdeneilanden ter voorkoming van oneerlijke of misleidende handelspraktijken over wetten die min of meer vergelijkbaar zijn met de Federal Trade Commission Act (FTC Act). FTC fact sheet, herdrukt in Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation, 59 Tul. L. Rev. 427 (1984). Een regulerende instantie is altijd bevoegd door middel van een dagvaarding of een civielrechtelijk verzoek terzake onderzoek te verrichten, van organisaties de garantie te verlangen dat zij de voorschriften vrijwillig naleven, bevel te geven bepaalde praktijken stop te zetten en om gerechtelijke bevelen te verkrijgen ter voorkoming van het gebruik van oneerlijke, onredelijke of misleidende handelspraktijken. Id. In 46 staten hebben particulieren de mogelijkheid om de werkelijke, een dubbele, een drievoudige of bij wijze van straf een zeer hoge schadevergoeding te eisen en in sommige gevallen ook vergoeding van de kosten en de honoraria van de advocaat. Id.

De Deceptive and Unfair Trade Practices Act uit Florida geeft de procureur-generaal bijvoorbeeld de bevoegdheid onderzoek te doen naar en civielrechtelijke procedures te beginnen wegens oneerlijke concurrentiemethoden en oneerlijke, onredelijke en misleidende handelspraktijken, waaronder onjuiste of misleidende advertenties, misleidende franchise- of zakelijke mogelijkheden, frauduleuze telemarketing en piramideprogramma's. Zie ook N.Y. General Business Law § 349 (waarbij oneerlijke handelingen en misleidende praktijken bij het zakendoen worden verboden).

Een enquête die dit jaar door de National Association of Attorneys General (NAAG) is gehouden, bevestigt deze bevindingen. De 43 staten die hebben geantwoord hebben allemaal „mini-FTC"-wetgeving of andere wetgeving die een vergelijkbare bescherming biedt. Bij dezelfde enquête gaven 39 staten aan dat zij klachten in ontvangst kunnen nemen van niet-ingezetenen. Ten aanzien van de particuliere levenssfeer van de consument in het bijzonder hebben 37 van de 41 staten die hebben geantwoord, aangegeven dat ze zouden reageren op klachten dat een bedrijf dat onder hun bevoegdheid valt, zich niet aan zijn eigen verklaringen ten aanzien van het privacybeleid zou houden.

BIJLAGE IV

Bescherming van de persoonlijke levenssfeer en schadevergoeding, wettelijke machtigingen en fusies en overnames in de wetgeving van de Verenigde Staten

Hiermee wordt voldaan aan het verzoek van de Europese Commissie om verduidelijking van de wetgeving van de Verenigde Staten met betrekking tot a) eisen tot schadevergoeding wegens inbreuken op de persoonlijke levenssfeer, b) „uitdrukkelijke machtigingen" in de wetgeving van de Verenigde Staten voor het gebruik van persoonsgegevens op een wijze die niet in overeenstemming is met de Veiligehavenbeginselen, en c) het effect van fusies en overnames op verplichtingen die op grond van de Veiligehavenbeginselen zijn aangegaan.

A. **Schadevergoeding wegens inbreuken op de persoonlijke levenssfeer**

Niet-naleving van de Veiligehavenbeginselen kan, afhankelijk van de omstandigheden, aanleiding geven tot een aantal particuliere vorderingen. Veiligehavenorganisaties kunnen met name aansprakelijk worden gesteld voor onjuiste verklaringen wanneer zij zich niet houden aan het door hen aangekondigde beleid inzake de bescherming van de persoonlijke levenssfeer. Particuliere gronden om een vordering tot schadevergoeding in te stellen wegens schendingen van de persoonlijke levenssfeer zijn ook voorhanden in het gewoonterecht. Voorts zijn er veel federale en staatswetten betreffende de persoonlijke levenssfeer die voorzien in de schadeloosstelling van particulieren wegens schendingen.

Het recht op schadeloosstelling wegens inbreuk op de persoonlijke levenssfeer is vast verankerd in het gewoonterecht van de Verenigde Staten.

Het gebruik van persoonsgegevens op een wijze die niet in overeenstemming is met de Veiligehavenbeginselen, kan op grond van een aantal verschillende rechtstheorieën leiden tot juridische aansprakelijkheid. Zo kunnen bijvoorbeeld zowel de voor de verwerking verantwoordelijke die informatie doorgeeft, als de betrokken personen tegen de veiligehavenorganisatie die haar veiligehavenverplichtingen niet nakomt, vervolging instellen wegens onjuiste verklaringen. Het Restatement of the Law, Second, Torts ([1]), bepaalt het volgende:

> Wie op bedrieglijke wijze een feit, mening, bedoeling of wet onjuist weergeeft met het doel een ander op basis daarvan te doen handelen of van handelen te weerhouden, kan tegenover de andere die is misleid, aansprakelijk worden gesteld voor geldelijk verlies dat deze heeft geleden doordat hij zich op verklaarbare wijze op de onjuiste weergave heeft gebaseerd.

Restatement, § 525. Een onjuiste weergave is „bedrieglijk" als ze geschiedt in de wetenschap of in de overtuiging dat ze verkeerd is. Id., § 526. In het algemeen is de maker van een onjuiste weergave tegenover iedereen van wie hij wil of verwacht dat hij zich op die onjuiste weergave zal baseren, potentieel aansprakelijk voor geldelijke verliezen die hij als gevolg daarvan kan lijden. Id. 531. Bovendien kan een persoon die op bedrieglijke wijze een onjuiste weergave doet tegenover een ander, tegenover een derde aansprakelijk worden gesteld indien de overtreder wil of verwacht dat zijn onjuiste weergave wordt herhaald tegenover de derde en dat deze daarnaar handelt. Id., § 533.

In het kader van de veilige haven is de desbetreffende weergave de openbare verklaring van de organisatie dat zij de Veiligehavenbeginselen zal naleven. Na het aangaan van een dergelijke verbintenis kan de bewuste niet-nakoming van de beginselen een reden zijn op grond waarvan een vordering wegens onjuiste verklaringen kan worden ingesteld door degenen die zich op de onjuiste verklaring hebben gebaseerd. Omdat de verbintenis om de beginselen na te leven tegenover het grote publiek wordt aangegaan, kunnen zowel de personen op wie deze informatie betrekking heeft, als de voor de verwerking verantwoordelijke in Europa die persoonsgegevens aan een organisatie in de Verenigde Staten doorgeeft, redenen hebben om tegen deze organisatie een vordering wegens onjuiste verklaringen in te stellen ([2]). Bovendien blijft de organisatie uit de Verenigde Staten tegenover hen aansprakelijk voor de „voortdurende onjuiste weergave" zolang zij zich in hun nadeel op de onjuiste weergave baseren. Restatement, § 535.

([1]) Second Restatement of the Law — Torts; American Law Institute (1997).

([2]) Dit kan bijvoorbeeld het geval zijn wanneer de personen op de verbintenissen van de Amerikaanse organisatie tot het naleven van de Veiligehavenbeginselen vertrouwden om aan de voor de verwerking verantwoordelijke toestemming te geven hun persoonsgegevens aan de Verenigde Staten door te geven.

Personen die zich op een bedrieglijke onjuiste weergave baseren, hebben recht op schadevergoeding. Het Restatement bepaalt het volgende:

> De ontvanger van een bedrieglijke onjuiste weergave heeft het recht om in een vordering wegens bedrog tegen de maker schadevergoeding te eisen voor het door hem geleden geldelijke verlies waarvan de onjuiste weergave de juridische oorzaak is.

Restatement, § 549. De in aanmerking komende schadevergoeding omvat het werkelijke contante verlies alsmede de gederfde „winst op de zaak" in een handelstransactie. Id.; zie bv. Boling v. Tennessee State Bank, 890 S.W.2d 32 (1994) (de bank is aan leners een bedrag van 14 825 USD verschuldigd als schadevergoeding voor het bekendmaken van persoonsgegevens en businessplannen van de leners aan de voorzitter van de bank, die een strijdig belang had).

Hoewel voor een bedrieglijke onjuiste weergave hetzij werkelijke kennis vereist is of ten minste de overtuiging dat de weergave verkeerd is, kan er ook aansprakelijkheid ontstaan wegens nalatige onjuiste weergave. Volgens het Restatement kan iedereen die tijdens de uitoefening van zijn zakelijke activiteit, beroepsbezigheid of dienstbetrekking of bij een geldelijke transactie een valse verklaring aflegt, aansprakelijk worden gesteld „als hij nalaat een redelijke zorgvuldigheid of bekwaamheid aan de dag te leggen bij het verkrijgen of mededelen van de informatie". Restatement, § 552(1). In tegenstelling tot wat bij bedrieglijke onjuiste weergave het geval is, is de schadevergoeding voor nalatige onjuiste weergave beperkt tot het contante verlies. Id., § 552B(1).

In een recente zaak bijvoorbeeld oordeelde het Superior Court van Connecticut dat het feit dat een elektriciteitsbedrijf had nagelaten bekend te maken dat het informatie betreffende klantenbetalingen aan nationale kredietinformatiebureaus rapporteerde, een grond was om een vordering wegens onjuiste weergave in te stellen. Zie Brouillard v. United Illuminating Co., 1999 Conn. Super. LEXIS 1754. In deze zaak werd de klager krediet geweigerd omdat de beklaagde betalingen die niet binnen 30 dagen na facturering werden ontvangen, als „achterstallig" rapporteerde. De klager voerde aan dat hij niet van dit beleid op de hoogte was gebracht toen hij bij de beklaagde een elektriciteitsaansluiting voor zijn woning aanvroeg. De rechtbank oordeelde meer specifiek dat „een vordering wegens nalatige onjuiste weergave kan worden gebaseerd op het feit dat de beklaagde nalaat te spreken wanneer het zijn plicht is dit te doen". Bijgevolg kan een organisatie uit de Verenigde Staten die verzuimt volledig bekend te maken hoe zij gebruik zal maken van persoonsgegevens die zij in het kader van de veilige haven ontvangt, wegens onjuiste weergave aansprakelijk worden gesteld.

In zoverre een schending van de Veiligehavenbeginselen misbruik van persoonsgegevens inhoudt, kan ze ook een grond vormen voor een vordering van de betrokkene wegens de onrechtmatige daad van gemeen recht die bestaat in een inbreuk op de persoonlijke levenssfeer. In het recht van de Verenigde Staten zijn sedert lang erkende gronden voor rechtsvorderingen betreffende inbreuken op de persoonlijke levenssfeer voorhanden. In een uit 1905 daterende zaak ([3]) achtte het Hooggerechtshof van Georgia een recht op persoonlijke levenssfeer dat zijn oorsprong vond in voorschriften van natuurrecht en gewoonterecht, van toepassing op een burger wiens foto door een levensverzekeringsmaatschappij voor het illustreren van een reclame was gebruikt zonder dat hij daarvoor zijn toestemming had gegeven of daarvan op de hoogte was. De rechtbank, die momenteel vertrouwde thema's in de jurisprudentie van de Verenigde Staten over de persoonlijke levenssfeer naar voren bracht, oordeelde dat het gebruik van de foto „kwaadwillig" en „vals" was en bedoeld om „klager voor de hele wereld belachelijk te maken" ([4]). De gronden van de Pavesich-beslissing zijn met lichte wijzigingen gehandhaafd en vormen nu de basis van de wetgeving van de Verenigde Staten op dit gebied. Staatsrechtbanken hebben op consequente wijze gronden voor rechtsvorderingen inzake inbreuken op de persoonlijke levenssfeer gesteund, en in ten minste 48 staten wordt nu een dergelijke grond voor een rechtsvordering juridisch erkend ([5]). Bovendien gelden in ten minste twaalf staten grondwettelijke bepalingen ter bescherming van het recht van hun burgers om gevrijwaard te blijven van indringerige handelingen ([6]), dat zich in sommige gevallen kan uitstrekken tot bescherming tegen indringing door niet-gouvernementele entiteiten. Zie bv. Hill v. NCAA, 865 P.2d 633 (Ca.1994); zie ook S. Ginder, Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet, 34 S.D. L. Rev. 1153 (1997) („Sommige staatsgrondwetten bieden een bescherming van de persoonlijke levenssfeer die verdergaat dan de bescherming van de persoonlijke levenssfeer in de grondwet van de Verenigde Staten. Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina en Washington bieden een ruimere bescherming van de persoonlijke levenssfeer.")

De Second Restatement of Torts biedt een gezaghebbend overzicht van het recht op dit gebied. In overeenstemming met de courante rechtspraktijk legt het Restatement uit dat het „recht op persoonlijke levenssfeer" vier verschillende gronden voor een vordering wegens onrechtmatige daad onder die noemer omvat. Zie Restatement, § 652A. Ten eerste kan een grond voor een vordering wegens „indringing bij afzondering" bestaan tegen een beklaagde die, fysiek of op

([3]) Pavesich v. New England Life Ins. Co., 50 S.E. 68(Ga. 1905).

([4]) Id. punt 69.

([5]) Een zoekvraag in de Westlaw-databank gaf als resultaat 2 703 gemelde gevallen van rechtszaken in staatsrechtbanken met betrekking tot de „persoonlijke levenssfeer" sinds 1995. Wij hebben de resultaten van deze zoekvraag reeds eerder aan de Commissie verstrekt.

([6]) Zie bv. Grondwet van Alaska, artikel 1, punt 22; Arizona, artikel 2, punt 8; California, artikel 1, punt 1; Florida, artikel 1, punt 23; Hawaii, artikel 1, punt 5; Illinois, artikel 1, punt 6; Louisiana, artikel 1, punt 5; Montana, artikel 2, punt 10; New York, artikel 1, punt 12; Pennsylvania, artikel 1, punt 1; South Carolina, artikel 1, punt 10; en Washington, artikel 1, punt 7.

andere wijze, opzettelijk binnendringt in de eenzaamheid of afzondering van een ander of in zijn privé-zaken of -aangelegenheden ([7]). Ten tweede kan er sprake zijn van een geval van „toe-eigening" wanneer men de naam of gelijkenis van een ander voor eigen gebruik of voordeel aanneemt ([8]). Ten derde kan tegen de „bekendmaking van privé-feiten" vervolging worden ingesteld als het bekendgemaakte materiaal van die aard is dat het voor een redelijke persoon zeer beledigend zou zijn en niet van rechtmatig belang voor het publiek ([9]). Ten slotte is een vordering wegens „publiciteit in vals daglicht" aangewezen wanneer de beklaagde bewust of onachtzaam een ander voor het publiek op zodanige wijze in een vals daglicht plaatst dat het voor een redelijke persoon zeer beledigend zou zijn ([10]).

In het kader van de veilige haven zou „indringing bij afzondering" het ongeoorloofde verzamelen van persoonsgegevens kunnen omvatten, terwijl het ongeoorloofde gebruik van persoonsgegevens voor commerciële doeleinden zou kunnen leiden tot een vordering wegens toe-eigening. Zo ook zou de bekendmaking van onjuiste persoonsgegevens neerkomen op een onrechtmatige daad die bestaat in „publiciteit in vals daglicht" als de gegevens als zeer beledigend voor een redelijke persoon kunnen worden aangemerkt. Ten slotte kan de inbreuk op de persoonlijke levenssfeer die het gevolg is van de bekendmaking of openbaarmaking van gevoelige persoonsgegevens een grond zijn voor een vordering wegens „bekendmaking van privé-feiten". (Zie voorbeelden van illustratieve gevallen hierna.)

Wat de schadevergoeding betreft, kunnen inbreuken op de persoonlijke levenssfeer de benadeelde het recht verlenen om schadevergoeding te eisen voor:

a) de door de inbreuk toegebrachte schade aan zijn belang in een persoonlijke levenssfeer;

b) zijn mentale leed waarvan is aangetoond dat het is ondergaan, als het van een soort is dat normaliter het gevolg van een dergelijke inbreuk is; en

c) bijzondere schade waarvan de inbreuk de juridische oorzaak is.

Restatement, § 652H. Gezien de algemene toepasselijkheid van het recht inzake onrechtmatige daad en de veelheid van gronden voor vorderingen betreffende verschillende aspecten van de bescherming van de persoonlijke levenssfeer, is het waarschijnlijk dat aan degenen die het slachtoffer worden van een schending van hun persoonlijke levenssfeer als gevolg van de niet-naleving van de Veiligehavenbeginselen, een geldelijke schadevergoeding wordt toegekend.

De staatsrechtbanken worden immers overstelpt met zaken wegens inbreuken op de persoonlijke levenssfeer in analoge situaties. Ex Parte AmSouth Bancorporation et al., 717 So. 2d 357, bijvoorbeeld betrof een collectief proces waarin werd aangevoerd dat de beklaagde „profiteerde van het vertrouwen dat de deposanten in de bank stelden door vertrouwelijke informatie betreffende de bankdeposanten en hun rekeningen mee te delen" teneinde een met de bank gelieerde maatschappij in staat te stellen gemeenschappelijke beleggingsfondsen en andere beleggingen te verkopen. In dergelijke gevallen wordt vaak schadevergoeding toegekend. In de zaak Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580 (D.C.App. 1985), vernietigde een hof van appèl een vonnis van een lagere rechtbank teneinde te beslissen dat het gebruik van foto's van de klager „vóór" en „na" plastische chirurgie tijdens een presentatie in een warenhuis een inbreuk op de persoonlijke levenssfeer wegens de bekendmaking van privé-feiten vormde. In de zaak Candebat v. Flanagan, 487 So.2d 207 (Miss. 1986), maakte de aangeklaagde verzekeringsmaatschappij in een reclamecampagne gebruik van een ongeval waarin de vrouw van de klager zwaargewond raakte. Klager stelde vervolging in wegens een schending van de persoonlijke levenssfeer. De rechtbank besliste dat klager recht had op schadevergoeding wegens emotioneel leed en toe-eigening van identiteit. Er kunnen vorderingen wegens wederrechtlijke toe-eigening worden ingesteld zelfs indien de klager niet persoonlijk beroemd is. Zie bv. Staruski v. Continental Telephone Co., 154 Vt. 568 (1990) (beklaagde haalde commercieel voordeel uit het gebruik van de naam en de foto van een werknemer in een krantenreclame). In de zaak Pulla v. Amoco Oil Co., 882 F.Supp. 836 (S.D. Iowa 1995), drong een werkgever binnen in de afzondering van beklaagde, een werknemer, door een andere werknemer opdracht te geven zijn creditcardgegevens na te trekken om zijn afwezigheden wegens ziekte te controleren. De rechtbank steunde een door een jury toegewezen feitelijke schadevergoeding van 2 USD en een als straf bedoelde schadevergoeding van 500 000 USD. Een andere werkgever werd aansprakelijk gesteld voor het bekendmaken van een verhaal in de bedrijfskrant over een werknemer die werd ontslagen omdat hij de gegevens betreffende zijn arbeidsverleden zou hebben vervalst. Zie Zinda v. Louisiana-Pacific Corp., 140 Wis.2d 277 (Wis.App. 1987). Het verhaal vormde door de bekendmaking van een privé-aangelegenheid een inbreuk op de persoonlijke levenssfeer van de klager omdat de krant in de gemeenschap werd verspreid. Ten slotte werd een universiteit die studenten op HIV testte nadat hun werd gezegd dat de bloedproef alleen bedoeld was om rode hond op te sporen, aansprakelijk gesteld voor indringing bij afzondering. Zie Doe v. High-Tech Institute, Inc., 972 P.2d 1060 (Colo.App. 1998). (Voor andere gemelde zaken, zie Restatement, § 652H, Appendix.)

De Verenigde Staten wordt vaak bekritiseerd omdat het te sterk tot procederen geneigd zou zijn, maar dit betekent ook dat particulieren echt rechtsmiddelen kunnen aanwenden, en dit ook doen, wanneer ze vinden dat hun onrecht is aan-

([7]) Id., hoofdstuk 28, punt 652B.
([8]) Id., hoofstuk 28, punt 652C.
([9]) Id., hoofdstuk 28, punt 652D.
([10]) Id., hoofdstuk 28, punt 652 E.

gedaan. Vele aspecten van het rechtssysteem van de Verenigde Staten maken het voor klagers gemakkelijk om hetzij individueel, hetzij gezamenlijk een proces aan te spannen. De balie, die verhoudingsgewijs groter is dan in de meeste andere landen, maakt professionele vertegenwoordiging gemakkelijk beschikbaar. Door klagers ingeschakelde advocaten die personen bij particuliere vorderingen vertegenwoordigen, werken doorgaans met een resultaatafhankelijke beloning, zodat zelfs arme of behoeftige klagers rechtsmiddelen kunnen aanwenden. Hiermee wordt een belangrijke factor naar voren gebracht — in de Verenigde Staten betaalt elke partij gewoonlijk het honorarium en andere kosten van haar eigen advocaat. In Europa daarentegen geldt als algemene regel dat de verliezende partij de kosten van de andere partij moet vergoeden. Zonder nader in te gaan op de relatieve voordelen van beide systemen kan worden gesteld dat met de in de Verenigde Staten geldende regel de kans kleiner is dat personen met rechtmatige vorderingen zich laten afschrikken omdat ze bang zijn de kosten van beide partijen niet te zullen kunnen betalen als ze het proces verliezen.

Personen kunnen een eis tot schadevergoeding instellen zelfs als hun vorderingen relatief klein zijn. In de meeste, zoniet alle staten van de Verenigde Staten zijn er rechtbanken voor kleine vorderingen die vereenvoudigde en minder dure procedures aanbieden voor geschillen die onder de wettelijke drempels blijven ([11]). De mogelijkheid dat een hoge schadevergoeding wordt toegewezen, biedt ook een financiële beloning aan personen die misschien weinig directe schade hebben geleden om vervolging wegens laakbaar wangedrag in te stellen. Ten slotte kunnen personen die op dezelfde wijze zijn benadeeld, hun middelen en hun vorderingen bundelen om een collectief proces aan te spannen.

Een goed voorbeeld van de mogelijkheid voor personen om een eis tot schadeloosstelling in te stellen is het hangende geschil tegen Amazon.com wegens inbreuk op de persoonlijke levenssfeer. Amazon.com, de grote on-linedetaillist, wordt aangeklaagd in een collectief proces waarbij de klagers beweren dat zij niet op de hoogte werden gebracht van, en niet hebben ingestemd met, het verzamelen van persoonsgegevens over hen toen zij gebruikmaakten van een softwareprogramma onder de naam „Alexa" dat eigendom is van Amazon. In deze zaak hebben de klagers gewezen op schendingen van de Computer Fraud and Abuse Act wegens illegale toegang tot hun opgeslagen communicaties, en van de Electronic Communications Privacy Act wegens illegale interceptie van hun elektronische en via kabel verzonden communicaties. Op grond van het gewoonterecht voeren zij tevens aan dat een schending van de persoonlijke levenssfeer heeft plaatsgevonden. Dit vloeit voort uit een klacht die in december door een deskundige op het gebied van Internetveiligheid werd ingediend. Er wordt een schadevergoeding van 1 000 USD per lid van de groep geëist, plus de honoraria van de advocaten en de winst die als gevolg van wetsovertredingen is gemaakt. Aangezien de groep miljoenen leden kan tellen, kan de totale schadevergoeding miljarden dollars bedragen. De FTC is ook bezig met een onderzoek van de beschuldigingen.

Federale en staatswetten inzake bescherming van de persoonlijke levenssfeer bieden particulieren vaak gronden voor het instellen van eisen tot geldelijke schadevergoeding.

Niet-naleving van de Veiligehavenbeginselen kan niet alleen leiden tot burgerlijke aansprakelijkheid op grond van het recht inzake onrechtmatige daad, maar kan ook een schending van een van de honderden federale en staatswetten inzake de persoonlijke levenssfeer vormen. Vele van deze wetten, die betrekking hebben op de verwerking van persoonsgegevens zowel door de overheid als de particuliere sector, stellen personen in staat om een eis tot schadevergoeding in te stellen wanneer overtredingen plaatsvinden. Bijvoorbeeld:

Electronic Communications Privacy Act van 1986. De ECPA verbiedt de ongeoorloofde interceptie van cellulaire telefoongesprekken en van datatransmissie tussen computers. Overtredingen kunnen leiden tot burgerlijke aansprakelijkheid met een geldboete van minimaal 100 USD per dag dat de overtreding duurt. De door de ECPA geboden bescherming strekt zich ook uit tot de ongeoorloofde toegang tot of bekendmaking van opgeslagen elektronische communicaties. Overtreders dienen de geleden schade te vergoeden of zien de winst die als gevolg van de overtreding is gemaakt, verbeurdverklaard.

Telecommunications Act van 1996. Krachtens hoofdstuk 702 mag klanteninformatie die eigendom is van telecommunicatienetten (CPNI, customer proprietary network information) niet worden gebruikt voor andere doeleinden dan het verlenen van telecommunicatiediensten. Abonnees van telecommunicatiediensten kunnen ofwel een klacht indienen bij de Federal Communications Commission, ofwel een proces aanhangig maken bij een federale arrondissementsrechtbank om schadevergoeding en de honoraria van de advocaten te vorderen.

Consumer Credit Reporting Reform Act van 1996. De wet van 1996 wijzigde de Fair Credit Reporting Act van 1970 (FCRA) teneinde verbetering te brengen in de kennisgeving en het recht van toegang betreffende kredietinformatiethema's. De herzieningswet legde ook nieuwe beperkingen op aan wederverkopers van consumentenkredietrapporten. Consumenten kunnen bij overtredingen schadevergoeding en de honoraria van de advocaten vorderen.

([11]) Wij hebben de Commissie reeds informatie over processen betreffende lage vorderingen verstrekt.

Staatswetten beschermen ook de persoonlijke levenssfeer in tal van situaties. Tot de gebieden waarop de staten maatregelen hebben genomen, behoren bankgegevens, abonnementen op kabeltelevisie, kredietrapporten, arbeidsgegevens, overheidsgegevens, genetische informatie en medische gegevens, verzekeringsgegevens, schoolgegevens, elektronische communicatie en videoverhuur ([12]).

B. **Uitdrukkelijke juridische machtigingen**

De Veiligehavenbeginselen bevatten een uitzondering wanneer wetten, regelingen of jurisprudentie „tegenstrijdige verplichtingen of uitdrukkelijke machtigingen creëren, mits de organisaties die van een dergelijke machtiging gebruikmaken kunnen aantonen dat de niet-naleving van de beginselen beperkt is tot de mate die nodig is om de met de machtiging beoogde doorslaggevende, legitieme belangen te waarborgen". Het is duidelijk dat, indien de wetgeving van de Verenigde Staten een tegenstrijdige verplichting oplegt, organisaties uit dat land de wet in acht moeten nemen, ongeacht of ze aan de veilige haven deelnemen of niet. Wat uitdrukkelijke machtigingen betreft, zijn we, ofschoon de Veiligehavenbeginselen bedoeld zijn om de verschillen tussen de regeling van de Verenigde Staten en die van de Europese Unie inzake bescherming van de persoonlijke levenssfeer te overbruggen, eerbied verschuldigd aan de prerogatieven van onze verkozen wetgevers op het gebied van wetgeving. De beperkte uitzondering op de strikte toepassing van de Veiligehavenbeginselen is bedoeld om een evenwicht tot stand te brengen tussen de legitieme belangen aan beide kanten.

De uitzondering is beperkt tot gevallen waar er een uitdrukkelijke machtiging voorhanden is. Daarom moet de desbetreffende wet, regeling of rechterlijke beslissing bij wijze van drempel het bijzondere gedrag van veiligehavenorganisaties affirmatief toestaan ([13]). Met andere woorden, de uitzondering zou niet gelden als de wet niet expliciet is. Bovendien zou de uitzondering alleen gelden als de uitdrukkelijke machtiging in strijd is met de naleving van de Veiligehavenbeginselen. Zelfs dan is de uitzondering „beperkt tot de mate die nodig is om de met de machtiging beoogde doorslaggevende, legitieme belangen te waarborgen". Om het duidelijk te stellen, wanneer de wet een onderneming gewoon machtigt persoonsgegevens aan overheidsinstanties te verstrekken, zou de uitzondering niet gelden. Omgekeerd, wanneer de wet de onderneming specifiek machtigt persoonsgegevens aan overheidsinstanties te verstrekken zonder de toestemming van de betrokkene, zou dit een „uitdrukkelijke machtiging" vormen om te handelen op een wijze die in strijd is met de Veiligehavenbeginselen. Aan de andere kant zouden specifieke uitzonderingen op affirmatieve voorschriften om kennisgeving te doen en toestemming te verkrijgen, binnen de uitzondering vallen (daar dit hetzelfde zou zijn als een specifieke machtiging om de informatie zonder kennisgeving en toestemming bekend te maken). Een wet bijvoorbeeld die artsen machtigt de medische gegevens over hun patiënten zonder voorafgaande toestemming van de patiënten aan ambtenaren van de gezondheidsdienst te verstrekken, zou een uitzondering op de beginselen van kennisgeving en keuze kunnen toelaten. Deze machtiging zou een arts niet toestaan dezelfde medische gegevens aan een organisatie voor gezondheidszorg (HMO, health maintenance organization) of aan commerciële farmaceutische onderzoekslaboratoria te verstrekken, wat buiten de door de wet toegestane doeleinden en bijgevolg buiten het geldingsgebied van de uitzondering zou vallen ([14]). Het rechtsinstrument in kwestie kan een „op zichzelf staande" machtiging zijn om specifieke dingen met persoonsgegevens te doen, maar, zoals uit de hierna gegeven voorbeelden blijkt, zal het waarschijnlijk een uitzondering op een ruimere wet zijn die het verzamelen, het gebruik of de bekendmaking van persoonsgegevens verbiedt.

Telecommunications Act van 1996

In de meeste gevallen is het toegestane gebruik ofwel in overeenstemming met de voorschriften van de richtlijn en de beginselen, ofwel wordt het gebruik door de een of andere erkende uitzondering toegestaan. Punt 702 van de Telecommunications Act (gecodificeerd in 47 U.S.C. § 222) legt telecommunicatie-exploitanten bijvoorbeeld de verplichting op de vertrouwelijkheid van persoonsgegevens die zij bij het verlenen van hun diensten aan hun klanten verkrijgen, in acht te nemen. Deze bepaling staat telecommunicatie-exploitanten specifiek toe:

1. klanteninformatie te gebruiken om telecommunicatiediensten te verlenen, inclusief de publicatie van telefoongidsen;

2. klanteninformatie op schriftelijk verzoek van de klant aan anderen te verstrekken; en

3. klanteninformatie in geaggregeerde vorm te verstrekken.

([12]) Een recente zoekvraag in de Westlaw-databank gaf als resultaat 994 gemelde zaken die in de staten werden behandeld en betrekking hadden op schadevergoeding en inbreuk op de privacy.

([13]) Ter verduidelijking zij erop gewezen dat het desbetreffende rechtsinstrument niet specifiek de Veiligehavenbeginselen zal hoeven aan te halen.

([14]) Zo ook zou de arts in dit voorbeeld zich niet op het wettelijke gezag kunnen baseren om geen rekening te houden met het recht van de betrokkene om te kiezen voor „opt-out" met betrekking tot direct marketing, zoals uiteengezet in FAQ 12. Het geldingsgebied van elke uitzondering voor „uitdrukkelijke machtigingen" is noodzakelijkerwijs beperkt tot het geldingsgebied van de machtiging op grond van de desbetreffende wet.

Zie 47 U.S.C. § 222(c)(1)-(3). De wet staat de telecommunicatie-exploitanten ook een uitzondering toe voor het gebruik van klanteninformatie om:

1. hun diensten in te leiden, te verlenen, de kosten daarvan te factureren en te innen;

2. te beschermen tegen bedrieglijk, beledigend of illegaal gedrag; en

3. telemarketing-, verwijs- of administratieve diensten te verlenen tijdens een oproep die door de klant tot stand is gebracht ([15]).

Id., § 222(d)(1)-(3). Ten slotte dienen de telecommunicatie-exploitanten informatie betreffende de abonneelijsten, die alleen de namen, adressen, telefoonnummers en de bedrijfsactiviteit voor commerciële klanten mag omvatten, aan uitgevers van telefoongidsen te verstrekken. Id., § 222(e).

De uitzondering voor „uitdrukkelijke machtigingen" zou een rol kunnen spelen wanneer telecommunicatie-exploitanten gebruikmaken van CPNI om bedrog of ander illegaal gedrag te voorkomen. Zelfs hier zouden dergelijke handelingen als van „openbaar belang" kunnen worden aangemerkt en om die reden door de beginselen kunnen worden toegelaten.

Regels voorgesteld door het ministerie van Volksgezondheid en Welzijn

Het ministerie van Volksgezondheid en Welzijn (HHS) heeft regels betreffende normen voor de bescherming van de persoonlijke levenssfeer ten aanzien van individueel identificeerbare gezondheidsinformatie voorgesteld. Zie 64 Fed. Reg. 59,918 (3 nov. 1999) (te codificeren in 45 C.F.R., punten 160-164). De regels zouden de voorschriften inzake de bescherming van de persoonlijke levenssfeer van de Health Insurance Portability and Accountability Act van 1996, Pub. L. 104-191, ten uitvoer leggen. De voorgestelde regels zouden de bedoelde entiteiten (d.w.z. gezondheidsplannen, clearingkantoren op het gebied van gezondheidszorg, en zorgverleners die gezondheidsinformatie in elektronisch formaat verzenden) in het algemeen verbieden beschermde gezondheidsinformatie zonder toestemming van de betrokkene te gebruiken of openbaar te maken. Zie het voorgestelde 45 C.F.R. § 164.506. Volgens de voorgestelde regels zou beschermde gezondheidsinformatie slechts voor twee doeleinden openbaar mogen worden gemaakt: 1. om de betrokkenen in staat te stellen de gezondheidsinformatie over henzelf te raadplegen en te kopiëren, zie id. § 164.514; en 2. om de regels te doen toepassen, zie id. § 164.522.

De voorgestelde regels zouden het gebruik of de openbaarmaking van beschermde gezondheidsinformatie zonder specifieke machtiging van de betrokkene in beperkte omstandigheden toestaan. Daaronder vallen bijvoorbeeld de inspectie van het gezondheidszorgstelsel, de rechtshandhaving en noodsituaties. Zie id. § 164.510. De voorgestelde regels beschrijven in detail de beperkingen die aan het gebruik en de openbaarmaking worden gesteld. Bovendien zouden het toegestane gebruik en de toegestane openbaarmaking van beschermde gezondheidsinformatie worden beperkt tot de minimale hoeveelheid benodigde informatie. Zie id. § 164.506.

Het gebruik dat door de voorgestelde regeling uitdrukkelijk wordt toegestaan, is in het algemeen in overeenstemming met de Veiligehavenbeginselen of wordt anders door een andere uitzondering toegestaan. Zo worden bijvoorbeeld rechtshandhaving en gerechtelijke administratie toegestaan, evenals medische research. Andere vormen van gebruik, zoals de inspectie van het gezondheidszorgstelsel, de functie volksgezondheid en door de overheid beheerde gezondheidsgegevenssystemen, dienen het openbaar belang. Openbaarmaking voor de verwerking van betalingen en premies in de gezondheidszorg is noodzakelijk voor het verlenen van gezondheidszorg. Het gebruik in noodsituaties, om de naaste verwanten te raadplegen in verband met een behandeling wanneer de toestemming van de patiënt „niet op een uitvoerbare of redelijke wijze kan worden verkregen", of om de identiteit of de doodsoorzaak van de overledene te bepalen, beschermt de vitale belangen van de betrokkene en van anderen. Het gebruik voor het beheer van militairen in actieve dienst of andere speciale categorieën personen draagt bij tot de behoorlijke uitvoering van de militaire taak of soortgelijke dringende situaties; en in elk geval zullen dergelijke vormen van gebruik weinig of niet van toepassing zijn op de consument in het algemeen.

Dan blijft alleen nog het gebruik van persoonsgegevens door instellingen voor gezondheidszorg om patiëntenlijsten te maken. Hoewel dit gebruik misschien niet het niveau van het „vitale" belang haalt, zijn de lijsten wel nuttig voor de patiënten en voor hun vrienden en verwanten. Bovendien is de reikwijdte van dit toegestane gebruik inherent zeer

([15]) Het geldingsgebied van deze uitzondering is zeer beperkt. Zoals deze is geformuleerd, kan de telecommunicatie-exploitant CPNI alleen gebruiken tijdens een oproep die door de klant tot stand is gebracht. Bovendien is ons door de FCC (Federal Communications Commission) medegedeeld dat de telecommunicatie-exploitant geen CPNI mag gebruiken om diensten te marketen die verdergaan dan datgene waar de klant om heeft verzocht. Ten slotte vormt deze bepaling eigenlijk helemaal geen „uitzondering", aangezien de klant moet instemmen met het gebruik van CPNI voor dit doel.

beperkt. Daarom vormt het inroepen van de uitzondering in de beginselen voor door de wet voor dit doel „uitdrukkelijk toegestane" vormen van gebruik een zeer gering risico voor de persoonlijke levenssfeer van patiënten.

Fair Credit Reporting Act

De Europese Commissie heeft er haar bezorgdheid over geuit dat de uitzondering voor „uitdrukkelijke machtigingen" „daadwerkelijk een vaststelling van gepastheid zou creëren" voor de Fair Credit Reporting Act (FCRA). Dit zou niet het geval zijn. Bij ontstentenis van een specifieke vaststelling van gepastheid voor de FCRA zouden de organisaties uit de Verenigde Staten die zich anders op een dergelijke vaststelling zouden baseren, moeten beloven de Veiligehavenbeginselen in alle opzichten na te leven. Dit betekent dat wanneer de FCRA-voorschriften het in de beginselen vastgelegde beschermingsniveau overtreffen, organisaties uit de Verenigde Staten alleen de FCRA hoeven na te leven. Omgekeerd, wanneer de FCRA te kort zou schieten, zouden die organisaties hun informatiepraktijken in overeenstemming met de beginselen moeten brengen. De uitzondering zou aan deze fundamentele beoordeling niets veranderen. Zoals de uitzondering is geformuleerd, geldt ze alleen wanneer de desbetreffende wet uitdrukkelijk gedrag toestaat dat niet met de Veiligehavenbeginselen in overeenstemming zou zijn. De uitzondering zou niet van toepassing zijn wanneer de FCRA-voorschriften gewoon niet beantwoorden aan de Veiligehavenbeginselen ([16]).

Met andere woorden, het ligt niet in onze bedoeling de uitzondering zo op te vatten dat wat niet wordt voorgeschreven, bijgevolg „uitdrukkelijk toegestaan" is. Bovendien geldt de uitzondering alleen wanneer datgene wat door de wetgeving van de Verenigde Staten uitdrukkelijk wordt toegestaan, in strijd is met de voorschriften van de Veiligehavenbeginselen. De wet in kwestie moet aan deze beide elementen voldoen voordat niet-naleving van de beginselen zou worden toegestaan.

Punt 604 van de FCRA bijvoorbeeld machtigt kredietinformatiebureaus uitdrukkelijk in verschillende opgesomde situaties consumentenrapporten uit te brengen. Zie FCRA, § 604. Als punt 604 aldus kredietinformatiebureaus machtigt in strijd met de Veiligehavenbeginselen te handelen, zouden de kredietinformatiebureaus zich op de uitzondering moeten baseren (tenzij natuurlijk een andere uitzondering zou gelden). Kredietinformatiebureaus moeten zich houden aan rechterlijke beslissingen en dagvaardingen voor de kamer van inbeschuldigingstelling, en het gebruik van kredietrapporten door overheidsdiensten voor wetshandhaving op het gebied van vergunningen, sociale bijstand en kinderbescherming dient een doel van openbaar belang. Id., § 604(a)(1), (3)(D) en (4). Bijgevolg zou het kredietinformatiebureau zich hiervoor niet op de uitzondering voor „uitdrukkelijke machtigingen" hoeven te baseren. Wanneer het kredietinformatiebureau handelt in overeenstemming met schriftelijke instructies van de consument, zou het volledig aan de Veiligehavenbeginselen voldoen. Id., § 604(a)(2). Zo kunnen ook consumentenrapporten worden verstrekt in verband met sollicitatieprocedures alleen met schriftelijke toestemming van de consument (id., §§ 604(a)(3)(B) en (b)(2)(A)(ii)) en met betrekking tot krediet- en verzekeringstransacties die niet op initiatief van de consument tot stand komen, alleen als de consument dergelijke verzoeken niet door een „opt-out" heeft geweigerd (id., § 604(c)(1)(B)). Voorts verbiedt de FCRA kredietinformatiebureaus medische informatie in verband met sollicitatieprocedures te verstrekken zonder de toestemming van de consument. Id., § 604(g). Dergelijke vormen van gebruik beantwoorden aan de beginselen van kennisgeving en keuze. Andere door punt 604 toegestane vormen van gebruik leiden tot transacties waarbij de consument betrokken is en zouden om die reden door de beginselen worden toegelaten. Zie id., § 604(a)(3)(A) en (F).

Het resternde door punt 604 „toegestane" gebruik heeft betrekking op secundaire kredietmarkten. Id., § 604(a)(3)(E). Het gebruik van consumentenrapporten voor dit doel is niet per se strijdig met de Veiligehavenbeginselen. Het is inderdaad zo dat de FRCA bijvoorbeeld niet van kredietinformatiebureaus verlangt dat ze kennisgeving doen aan en toestemming verkrijgen van de consumenten wanneer ze rapporten voor dat doel verstrekken. Wij wijzen er echter nogmaals op dat de afwezigheid van een verplichting niet neerkomt op een „uitdrukkelijke machtiging" om op een andere wijze te handelen dan wordt verlangd. Zo staat ook punt 608 kredietinformatiebureaus toe sommige persoonsgegevens aan overheidsdiensten te verstrekken. Deze „machtiging" zou niet rechtvaardigen dat een kredietinformatiebureau zich niet houdt aan zijn verplichtingen om de Veiligehavenbeginselen na te leven. Dit staat in tegenstelling tot onze andere voorbeelden waar uitzonderingen op affirmatieve verplichtingen inzake kennisgeving en keuze gelden om het gebruik van persoonsgegevens zonder kennisgeving en keuze uitdrukkelijk toe te staan.

Conclusie

Zelfs onze beperkte bespreking van deze wetten levert een duidelijk patroon op:

— de „uitdrukkelijke machtiging" in de wet staat in het algemeen het gebruik of de openbaarmaking van persoonsgegevens zonder voorafgaande toestemming van de betrokkene toe; de uitzondering zou bijgevolg beperkt blijven tot de beginselen van kennisgeving en keuze;

([16]) Onze bespreking hier mag niet worden opgevat als een erkenning dat de FCRA geen „passende" bescherming biedt. Bij elke beoordeling van de FCRA moet de door de wet geboden bescherming in haar geheel worden beschouwd en mag niet alleen naar de uitzonderingen worden gekeken, zoals wij hier doen.

— in de meeste gevallen zijn de door de wet toegestane uitzonderingen scherp omlijnd en bedoeld om in specifieke situaties voor specifieke doeleinden te worden toegepast. In alle gevallen verbiedt de wet overigens het ongeoorloofde gebruik of de ongeoorloofde openbaarmaking van persoonsgegevens die niet binnen deze grenzen vallen;

— in de meeste gevallen dient het toegestane gebruik of de toegestane openbaarmaking een openbaar belang, waarin het wetgevende karakter ervan tot uiting komt;

— in bijna alle gevallen is het toegestane gebruik ofwel volledig in overeenstemming met de Veiligehavenbeginselen, ofwel valt het onder de een of andere toegestane uitzondering.

Tot besluit kan worden gesteld dat de uitzondering voor „uitdrukkelijke machtigingen" in de wet uit de aard der zaak waarschijnlijk een vrij beperkte draagwijdte zal hebben.

C. **Fusies en overnames**

De Groep van artikel 29 heeft zijn bezorgdheid uitgedrukt over situaties waarin een organisatie die aan de veilige haven deelneemt, wordt overgenomen door of fuseert met een onderneming die zich er niet toe heeft verbonden de Veiligehavenbeginselen na te leven. De Groep lijkt echter te hebben aangenomen dat de overblijvende onderneming niet verplicht zou zijn de Veiligehavenbeginselen toe te passen op persoonsgegevens in het bezit van de onderneming die wordt overgenomen, maar dat is niet noodzakelijk het geval volgens de wetgeving van de Verenigde Staten. De algemene regel in de Verenigde Staten wat fusies en overnames betreft, is dat een onderneming die het uitstaande aandelenkapitaal van een andere onderneming verwerft, in het algemeen de verplichtingen en lasten van het overgenomen bedrijf mede overneemt. Zie 15 Fletcher Cyclopedia of the Law of Private Corporations § 7117 (1990); zie ook Model Bus. Corp. Act § 11.06(3) (1979) („de overblijvende onderneming draagt alle lasten van elke onderneming die partij is bij de fusie"). Met andere woorden, de overblijvende onderneming bij een fusie met of overname van een veiligehavenorganisatie zou volgens deze methode de veiligehavenverbintenissen van deze laatste moeten nakomen.

Bovendien is het zo dat, zelfs indien de fusie of overname zou geschieden door de verwerving van activa, de verplichtingen van de overgenomen onderneming niettemin het overnemende bedrijf in bepaalde omstandigheden kunnen binden. 15 Fletcher, § 7122. Overigens zij erop gewezen dat, zelfs indien de verplichtingen niet zouden blijven bestaan na de fusie, zij evenmin zouden blijven bestaan na een fusie waarbij de gegevens uit Europa waren doorgegeven op grond van een overeenkomst — het enige mogelijke alternatief voor de veilige haven voor gegevensoverdrachten naar de Verenigde Staten. Bovendien is elke veiligehavenorganisatie nu op grond van de veiligehavendocumenten in de herziene versie verplicht het ministerie van Handel in kennis te stellen van elke overname en mogen gegevens alleen verder aan de overnemende organisatie worden doorgegeven als de overnemende organisatie tot de veilige haven toetreedt. Zie FAQ 6. De Verenigde Staten heeft nu immers het veiligehavenkader herzien zodat organisaties uit dat land in deze situatie verplicht zijn informatie te wissen die zij in het kader van de veilige haven hebben ontvangen, als hun veiligehavenverbintenissen niet blijven bestaan of geen andere geschikte waarborgen worden geboden.

BIJLAGE V

14 juli 2000

De heer John Mogg
Directeur-generaal
DG Interne markt
Europese Commissie
Kamer C 107-6/72
Wetstraat 200
B-1049 Brussel

Geachte heer Mogg,

Ik begrijp dat er een aantal vragen is gerezen naar aanleiding van mijn brief aan u van 29 maart 2000. Om duidelijk te maken wat onze bevoegdheden zijn op de gebieden waarop u vragen stelt, stuur ik u deze brief. Met het oog op latere verwijzingen recapituleer ik een deel van de tekst van eerdere correspondentie, en geef ik hierop een aanvulling.

Tijdens uw bezoeken aan ons en in uw correspondentie heeft u diverse vragen over de bevoegdheden van de Federal Trade Commission op het gebied van de bescherming van de persoonlijke levenssfeer bij het on-lineverkeer van informatie aan de orde gesteld. Het leek mij nuttig mijn eerdere antwoorden samen te vatten en aanvullende informatie te verschaffen over de competentie van de FTC op het gebied van de bescherming van de persoonlijke levenssfeer van de consument, die u in uw laatste brief aan de orde stelt. Met name vraagt u of: 1. de FTC bevoegd is wanneer personeelsgegevens in strijd met de Veiligehavenbeginselen van de Verenigde Staten worden doorgegeven; 2. de FTC bevoegd is voor programma's zonder winstoogmerk waarbij keurmerken voor de bescherming van de persoonlijke levenssfeer worden verleend; 3. de FTC Act zowel op on-line- als op off-linegegevens van toepassing is; en 4. wat er gebeurt wanneer de bevoegdheden van de FTC die van andere met de rechtshandhaving belaste instanties overlappen.

Toepassing van de FTC Act op de bescherming van de persoonlijke levenssfeer

De wettelijke bevoegdheden van de Federal Trade Commission op dit gebied zijn te vinden in sectie 5 van de Federal Trade Commission Act („FTC Act"), die oneerlijke of misleidende handelingen of praktijken in het handelsverkeer verbiedt [1]. Een misleidende praktijk is een voorstelling van zaken, een omissie of een handeling die waarschijnlijk tot gevolg heeft dat verstandige consumenten op belangrijke punten worden misleid. Een praktijk is oneerlijk wanneer deze consumenten aanzienlijke schade toebrengt of kan toebrengen, die redelijkerwijze niet kan worden vermeden en die niet wordt gecompenseerd door voordelen voor de consumenten of de concurrentie [2].

Bepaalde praktijken bij de verzameling van informatie vormen waarschijnlijk een overtreding van de FTC Act. Wanneer bijvoorbeeld op een website ten onrechte wordt gezegd dat men zich aan een officieel beleid inzake de bescherming van de persoonlijke levenssfeer of aan een reeks zelfreguleringsrichtlijnen houdt, biedt sectie 5 van de FTC Act een rechtsgrond om zo'n onjuiste voorstelling van zaken als misleiding aan te vechten. Wij zijn er inderdaad in geslaagd om de wet op zodanige wijze toe te passen dat dit beginsel vastligt [3]. Bovendien heeft de Commissie het standpunt ingenomen dat zij uit hoofde van sectie 5 bijzonder flagrante praktijken op het gebied van de bescherming van de persoonlijke levenssfeer kan aanvechten indien hierbij kinderen zijn betrokken of het gebruik van zeer gevoelige informatie zoals financiële gegevens [4] en medische dossiers. De FTC zal zich blijven inspannen voor rechtshandhaving door middel van actief toezicht en onderzoek en via de zaken die haar worden voorgelegd door zelfregulerende organisaties en anderen, waaronder de lidstaten van de Europese Unie.

---

[1] Titel 15 van de U.S.C., sectie 45. Ook de Fair Credit Reporting Act kan van toepassing zijn op de verzameling en verkoop van internetgegevens die voldoen aan de wettelijke definities van „rapport over consumenten"en „instantie die rapporten over consumenten opstelt".

[2] Titel 15 van de U.S.C., sectie 45(n).

[3] Zie GeoCities, Docket No. C-3849 (eindvonnis van 12 februari 1999) (beschikbaar op www.ftc.gov/os/1999/9902/9823015d%26o.htm); Liberty Financial Cos., Docket No. C-3891 (eindvonnis van 12 augustus 1999) (beschikbaar op www.ftc.gov/opa/1999/9905/younginvestor.htm). Zie ook Children's Online Privacy Protection Act Rule (COPPA), 16 C.F.R. Part 312 (beschikbaar op www.ftc.gov/opa/1999/9910/childfinal.htm). De COPPA-beslissing die afgelopen maand van kracht werd, verplicht exploitanten van websites die zijn gericht op kinderen tot 13 jaar of die bewust persoonsgegevens van kinderen tot 13 jaar verzamelen, ertoe de in de beslissing genoemde normen inzake een eerlijke informatiepraktijk toe te passen.

[4] Zie FTC v. Touch Tone, Inc., Civil Action No. 99-WM-783 (D.Co.) (geklasseerd op 21 april 1999), www.ftc.gov/opa/1999/9904/touchtone.htm. Staff Opinion Letter, 17 juli 1997, naar aanleiding van een klacht van het Center for Media Education, www.ftc.gov/os/1997/9707/cenmed.htm.

Ondersteuning van zelfregulering

De FTC zal prioriteit geven aan zaken betreffende niet-nakoming van zelfreguleringsrichtsnoeren, die haar door organisaties als BBBOnline en TRUSTe worden voorgelegd ([5]). Deze aanpak is in overeenstemming met onze langdurige relatie met de National Advertising Review Board (NARB) of het Better Business Bureau, dat klachten over reclame aan de FTC voorlegt. De National Advertising Division (NAD) van de NARB arbitreert bij klachten over nationale reclamecampagnes. Wanneer een partij weigert gevolg te geven aan het besluit van de NAD wordt de zaak aan de FTC voorgelegd. Het FTC-personeel onderzoekt de aangevochten reclame zo snel mogelijk om vast te stellen of deze in strijd is met de FTC Act, en vaak lukt het het aangevochten gedrag te stoppen of het betrokken bedrijf ervan te overtuigen weer aan het NARB-proces deel te nemen.

De FTC zal op dezelfde wijze ook prioriteit geven aan klachten over niet-nakoming van de Veiligehavenbeginselen uit de lidstaten van de Europese Unie. Evenals bij verzoeken van zelfregulerende organisaties uit de Verenigde Staten zullen onze medewerkers rekening houden met alle informatie aan de hand waarvan kan worden vastgesteld of het aangeklaagde gedrag in strijd is met sectie 5 van de FTC Act. Deze toezegging is ook te vinden in de Veiligehavenbeginselen, bij de Frequently Asked Question (FAQ 11) over handhaving.

GeoCities: De eerste zaak van de FTC over de bescherming van de persoonlijke levenssfeer op internet

De eerste zaak van de FTC over de bescherming van de persoonlijke levenssfeer op internet, GeoCities, berustte op de bevoegdheden van de Commissie uit hoofde van sectie 5 ([6]). In die zaak beweerde de FTC dat GeoCities tegenover zowel volwassenen als kinderen een verkeerde voorstelling van zaken gaf van de wijze waarop hun persoonsgegevens zouden worden gebruikt. Volgens de FTC deed GeoCities alsof bepaalde persoonlijke informatie die het op zijn website verzamelde, alleen zou worden gebruikt voor interne doeleinden of om de consumenten speciale aanbiedingen te doen voor producten of diensten die zij verlangden, en dat bepaalde aanvullende „facultatieve" informatie aan niemand zou worden bekendgemaakt zonder toestemming van de consument. In feite werd deze informatie doorgegeven aan derden, die deze gebruikten om de consumenten te bestoken met reclame die veel verder ging dan waarvoor zij toestemming hadden gegeven. Ook werd GeoCities van misleiding met betrekking tot de verzameling van informatie bij kinderen beschuldigd. Volgens de klacht van de FTC deed GeoCities alsof het op zijn website een kinderhoekje exploiteerde en dat de daar verzamelde informatie onder haar hoede zou blijven. In feite werden deze gebieden op de website door derden beheerd, die deze informatie verzamelden en onder zich hielden.

In de regeling die werd getroffen, werd GeoCities verboden een onjuiste voorstelling van zaken te geven ten aanzien van het doel waarvoor het persoonsgegevens van of over consumenten, inclusief kinderen, verzamelt of gebruikt. Het bedrijf moest op zijn website duidelijk en prominent een mededeling over de bescherming van de persoonlijke levenssfeer plaatsen, waarin de consumenten wordt gezegd welke informatie wordt verzameld en waarvoor, aan wie deze zal worden bekendgemaakt en hoe de consumenten toegang tot deze informatie kunnen krijgen en deze kunnen verwijderen. Om ervoor te zorgen dat ouders kunnen controleren wat hun kinderen doen, moet GeoCities voorts de toestemming van de ouders inwinnen voordat persoonsgegevens over kinderen van twaalf jaar en jonger worden verzameld. Verder moest GeoCities haar leden hiervan in kennis stellen en hun de mogelijkheid geven informatie over zichzelf uit de databanken van GeoCities en eventuele derden te verwijderen. Meer in het bijzonder moest GeoCities ouders van kinderen van twaalf jaar of jonger op de hoogte brengen en informatie over hen wissen, tenzij een van de ouders zou bevestigen dat de informatie mag worden gehouden en gebruikt. Ten slotte werd GeoCities verplicht contact op te nemen met de derden aan wie het voorheen de informatie bekendmaakte en hun te vragen deze informatie te wissen ([7]).

ReverseAuction.com

In januari 2000 verklaarde de FTC een klacht tegen ReverseAuction.com gegrond en bereikte zij een schikking met dit bedrijf, een internet-veilingsite die via een concurrerende site (eBay.com) persoonsgegevens over consumenten zou hebben gekregen en vervolgens misleidende, ongevraagde e-mailberichten zou hebben gezonden naar consumenten die zaken wilden doen ([8]). De FTC stelde dat ReverseAuction sectie 5 van de FTC Act overtrad toen het de persoonsgege-

([5]) Onlangs nog heeft de FTC bij een federale rechtbank een klacht tegen een houder van een TRUSTe-keurmerk, Toysmart.com, ingediend, teneinde te voorkomen dat vertrouwelijke, persoonlijke informatie over klanten, die het bedrijf op zijn website had verzameld, in strijd met het eigen privacybeleid zou worden verkocht. De FTC werd rechtstreeks door TRUSTe op de hoogte gesteld van deze mogelijke wetsovertreding. FTC v. Toysmart.com, LLC, Civil Action No. 00-11341-RGS (D.Ma.) (ingediend op 11 juli 2000) (beschikbaar op www.ftc.gov/opa/2000/07/toysmart.htm).

([6]) GeoCities, Docket No. C-3849 (eindvonnis van 12 februari 1999) (beschikbaar op www.ftc.gov/os/1999/9902/9823015d%26o.htm).

([7]) Nadien behandelde de Commissie nog een andere zaak over de verzameling van persoonsgegevens van kinderen op internet. Liberty Financial Companies, Inc., exploiteerde de „Young Investor"-website die op kinderen en tieners was gericht en waarin onderwerpen met betrekking tot geld en investeren centraal stonden. De FTC beweerde dat in een enquête bij kinderen verzamelde persoonsgegevens anoniem zouden worden bewaard en dat de deelnemers per e-mail een nieuwsbrief zouden krijgen, alsmede prijzen. In werkelijkheid werden de persoonsgegevens over het kind en de gezinsfinanciën op identificeerbare wijze opgeslagen, terwijl er ook geen nieuwsbrief of prijzen werden gezonden. In de schikking werd een dergelijke onjuiste voorstelling van zaken in de toekomst verboden; Liberty Financial moet een mededeling over de bescherming van de persoonlijke levenssfeer op zijn sites voor kinderen plaatsen en verifieerbare toestemming van de ouders krijgen voordat persoonsgegevens van kinderen worden verzameld. Liberty Financial Cos., Docket No. C-3891 (eindvonnis van 12 augustus 1999) (beschikbaar op www.ftc.gov/opa/1999/9905/younginvestor.htm).

([8]) Zie ReverseAuction.com, Inc., Civil Action No. 000032 (D.D.C.) (geregistreerd op 6 januari 2000) (persbericht en pleidooien op www.ftc.gov/opa/2000/01/reverse4.htm).

vens, waaronder de e-mailadressen van de eBay-gebruikers en hun persoonlijke identificatie („user IDs"), kreeg en misleidende e-mailboodschappen stuurde.

Zoals in de aanklacht wordt beschreven, schreef ReverseAuction zich, om informatie te verkrijgen, als eBay-gebruiker in en beloofde het zich te houden aan de verkoopvoorwaarden en het beleid van eBay inzake de bescherming van de persoonlijke levenssfeer. Deze hebben ten doel de persoonlijke levenssfeer van consumenten te beschermen doordat het eBay-gebruikers wordt verboden persoonsgegevens te verzamelen en te gebruiken voor niet-toegestane doeleinden, zoals het zenden van ongevraagde commerciële e-mailberichten. In onze aanklacht werd dus primair gesteld dat ReverseAuction een verkeerde voorstelling van zaken gaf toen het beweerde zich aan de verkoopvoorwaarden en het beleid van eBay inzake de bescherming van de persoonlijke levenssfeer te zullen houden, wat neerkomt op een misleidende praktijk in de zin van sectie 5. Subsidiair stelde de aanklacht dat het gebruik van de informatie door ReverseAuction om in strijd met de verkoopvoorwaarden en het beleid inzake de bescherming van de persoonlijke levenssfeer ongevraagd commerciële e-mail te sturen een oneerlijke handelspraktijk ingevolge sectie 5 betekende.

Ten tweede stond in de aanklacht dat de e-mailberichten aan de consumenten een onjuist onderwerp vermeldden: hun werd gezegd dat hun user ID voor eBay „weldra verloopt". Ten slotte stelde de aanklacht dat de e-mailberichten er ten onrechte gewag van maakten dat eBay ReverseAuction direct of indirect de persoonsgegevens van de eBay-gebruikers verstrekte dan wel op andere wijze deel had aan de verspreiding van de ongevraagde e-mail.

De FTC oordeelde dat ReverseAuction dergelijke overtredingen in de toekomst niet meer mocht begaan. Ook moest ReverseAuction de consumenten die zich naar aanleiding van zijn e-mail bij hem hadden geregistreerd of dit nog zullen doen, meedelen dat hun user ID bij eBay niet verloopt en dat eBay niets wist van de verspreiding van ongevraagde e-mail door ReverseAuction en dit ook niet billijkte. Verder moesten de consumenten op de hoogte worden gesteld van de mogelijkheid de registratie bij ReverseAuction te wissen en hun persoonsgegevens uit de databank van ReverseAuction te verwijderen. Bovendien moest ReverseAuction de persoonsgegevens van eBay-leden die de e-mail van ReverseAuction weliswaar hadden ontvangen, maar daar niet waren geregistreerd, wissen en ervan afzien deze te gebruiken of bekend te maken. Evenals in andere zaken inzake de bescherming van de persoonlijke levenssfeer bepaalde de FTC ook in deze zaak dat ReverseAuction zijn beleid terzake op zijn internetsite bekend moest maken en dat het een uitgebreid register moest bijhouden, zodat de FTC kan nagaan of het bedrijf het vonnis ook uitvoert.

Uit de zaak ReverseAuction blijkt dat de FTC zich ervoor inzet dwangmaatregelen te gebruiken om de zelfreguleringsinspaningen van het bedrijfsleven op het gebied van de bescherming van de persoonlijke levenssfeer van de consumenten op internet te ondersteunen. In deze zaak werd immers gedrag dat het beleid en de verkoopvoorwaarden ter bescherming van de persoonlijke levenssfeer van de consumenten ondermijnde en het consumentenvertrouwen in de maatregelen van internetbedrijven terzake zou kunnen aantasten, aan de kaak gesteld. Omdat het ging om de wederrechtelijke toe-eigening door een bedrijf van consumenteninformatie die werd beschermd door het beleid inzake de bescherming van de persoonlijke levenssfeer van een ander bedrijf, kan het ook van groot belang zijn bij de bescherming van de persoonlijke levenssfeer in het kader van de doorgifte van gegevens tussen bedrijven in verschillende landen.

Niettegenstaande deze acties van de FTC op het gebied van de rechtshandhaving in de zaken GeoCities, Liberty Financial Cos. en ReverseAuction zijn haar bevoegdheden op sommige gebieden van de bescherming van de persoonlijke levenssfeer op het net beperkter. Zoals hierboven al is opgemerkt, valt de verzameling en het gebruik van persoonsgegeven zonder toestemming alleen dan onder de FTC Act wanneer het gaat om een misleidende of oneerlijke handelspraktijk. Met de FTC Act kan dus waarschijnlijk niets worden gedaan tegen praktijken van een website die persoonsgegevens van klanten verzamelt, maar geen onjuiste voorstelling van zaken geeft van het doel waarvoor de informatie wordt verzameld of die de gegevens op zodanige wijze gebruikt of vrijgeeft dat de klanten hiervan waarschijnlijk geen grote schade zullen ondervinden. Het ligt momenteel waarschijnlijk ook niet op de weg van de FTC om in het algemeen van organisaties die informatie op internet verzamelen te eisen dat zij zich aan een beleid inzake de bescherming van de persoonlijke levenssfeer in het algemeen of aan een specifiek beleid terzake houden ([9]). Overigens is er, zoals hierboven al is gezegd, waarschijnlijk sprake van misleiding wanneer een bedrijf zich niet aan zijn eigen beleid inzake de bescherming van de persoonlijke levenssfeer houdt.

([9]) Daarom verklaarde de FTC in een getuigenverklaring voor het Congres dat waarschijnlijk extra wetgeving nodig is om alle commerciële websites in de Verenigde Staten die op consumenten gericht zijn, te verplichten zich te houden aan gespecificeerde praktijken inzake eerlijke informatie. „Consumer Privacy on the World Wide Web" voor het Subcomité voor Telecommunicatie, handel en consumentenbescherming van het Comité van het Huis van Afgevaardigden voor de handel, 21 juli 1998 (getuigenis kan worden gevonden op www.ftc.gov/os/9807/privac98.htm). De FTC heeft met haar oproep voor dergelijke wetgeving gewacht om het bedrijfsleven de mogelijkheid te bieden aan te tonen dat het ook door zelfregulering kan komen tot een wijdverbreide aanvaarding van praktijken inzake eerlijke informatie op websites. In het rapport van de FTC aan het Congres over de bescherming van de persoonlijke levenssfeer op internet, „Privacy Online: A Report to Congress", juni 1998 (het rapport is te vinden op www.ftc.gov/reports/privacy3/toc.htm), deed de FTC een aanbeveling voor wetgeving om commerciële websites te verplichten instemming van de ouders te verkrijgen voordat persoonsgegevens bij kinderen tot 13 jaar worden verzameld. Zie voetnoot 3. Afgelopen jaar bleek uit het FTC-rapport „Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress" van juli 1999 (te vinden op www.ftc.gov/os/1999/9907/index.htm#13) dat er sprake was van voldoende vooruitgang bij de zelfregulering, zodat de FTC op dat moment geen wetgeving terzake wilde aanbevelen. In mei 2000 heeft de FTC haar derde rapport, „Privacy Online: Fair Information Practices in the Electronic Marketplace", (te vinden op www.ftc.gov/os/2000/05/index.htm#22) voorgelegd aan het Congres. Hierin wordt gesproken over recent onderzoek van de FTC naar commerciële websites en hun naleving van eerlijke informatiepraktijken. Het rapport geeft ook een aanbeveling (onderschreven door een meerderheid van de FTC) aan het Congres wetgeving inzake een basisniveau voor de bescherming van de persoonlijke levenssfeer op op de consument gerichte commerciële websites uit te vaardigen.

Verder strekken de bevoegdheden van de FTC op dit gebied zich enkel uit tot oneerlijke of misleidende handelingen of praktijken die betrekking hebben op de handel. Het verzamelen van informatie door commerciële bedrijven die reclame maken voor goederen of diensten of die voor commerciële doeleinden informatie verzamelen en gebruiken, valt waarschijnlijk onder dit handelsvereiste. Anderzijds zijn er waarschijnlijk veel particulieren of bedrijven die informatie op het net verzamelen zonder commercieel doel en daardoor niet onder de jurisdictie van de FTC vallen. Een voorbeeld van deze beperking betreft de zogenaamde „chat rooms" indien deze worden geëxploiteerd door niet-commerciële instanties zoals charitatieve organisaties.

Ten slotte zijn er een aantal volledige of gedeeltelijke wettelijke uitzonderingen op de basisbevoegdheden van de FTC inzake commerciële praktijken, waardoor de FTC niet altijd kan reageren op kwesties betreffende de bescherming van de persoonlijke levenssfeer op internet. Hiertoe behoren uitzonderingen ten aanzien van veel informatie-intensieve bedrijven zoals banken, verzekeringsmaatschappijen en luchtvaartmaatschappijen. Zoals u weet, vallen deze bedrijven onder de jurisdictie van andere federale instanties dan wel instanties van de deelstaten, bijvoorbeeld de Federale Bankautoriteiten en het ministerie van Vervoer.

In de gevallen waarin de FTC zelf bevoegd is, accepteert zij en, voorzover haar middelen dit toelaten, treedt zij op bij klachten die zij in haar Consumer Response Center („CRC") per post of telefoon en sinds kort ook via haar website ([10]) van consumenten ontvangt. Het CRC accepteert klachten van alle consumenten, ook als dezen in de lidstaten van de Europese Unie wonen. Op grond van de FTC Act is de FTC als onpartijdige instantie bevoegd om bij overtredingen van de FTC Act dwangmaatregelen op te leggen en een schadeloosstelling vast te stellen voor consumenten die schade hebben geleden. De FTC moet evenwel nagaan of het bedrijf in kwestie zich voortdurend onoorbaar gedraagt omdat zij geen individuele klachten van consumenten behandelt. In het verleden heeft de FTC schadeloosstelling vastgesteld voor burgers uit de Verenigde Staten en uit andere landen ([11]). De FTC zal haar bevoegdheid in de aangewezen gevallen blijven gebruiken om schadeloosstelling te verkrijgen voor burgers uit andere landen die schade hebben geleden door misleidende praktijken die onder haar bevoegdheid vallen.

Personeelsgegevens

In uw laatste brief vroeg u nadere informatie over de bevoegdheid van de FTC op het gebied van personeelsgegevens. Eerst stelt u de vraag of de FTC in het kader van sectie 5 actie kan ondernemen tegen een bedrijf dat voorgeeft zich aan de Veiligehavenbeginselen van de Verenigde Staten te houden, maar dat personeelsgegevens doorgeeft of gebruikt op een wijze die in strijd is met deze beginselen. Wij willen u de verzekering geven dat wij de wetgeving over de bevoegdheden van de FTC, aanverwante documentatie en de desbetreffende jurisprudentie zorgvuldig hebben onderzocht en tot de conclusie zijn gekomen dat de FTC voor personeelsgegevens dezelfde jurisdictie heeft als zij in het algemeen ingevolge sectie 5 van de FTC Act heeft ([12]). Wanneer we ervan uitgaan dat een zaak voldoet aan onze huidige criteria voor een dwangmaatregel op het gebied van de bescherming van de persoonlijke levenssfeer (oneerlijkheid of misleiding), betekent dit dat we actie kunnen ondernemen indien het gaat om personeelsgegevens.

Ook willen wij erop wijzen dat de FTC zeker niet alleen dan actie op het gebied van de bescherming van de persoonlijke levenssfeer kan ondernemen wanneer een bedrijf individuele klanten heeft misleid. Zoals de recente actie van de FTC in de zaak ReverseAuction ([13]) heeft duidelijk gemaakt, zal de FTC dergelijke maatregelen nemen in gevallen waarin een bedrijf bij de doorgifte van gegevens tussen bedrijven onwettig heeft gehandeld jegens een ander bedrijf, waarbij zowel voor de consumenten als voor de bedrijven schade kan zijn ontstaan. Wij nemen aan dat personeelskwesties vooral in dergelijke zaken aan de orde komen, daar personeelsgegevens over Europeanen vanuit Europese bedrijven worden doorgegeven aan bedrijven uit de Verenigde Staten die hebben beloofd zich aan de Veiligehavenbeginselen te houden.

Wij willen evenwel wijzen op één omstandigheid waarin de actie van de FTC beperkt zal zijn. Dit betreft gevallen waarin de zaak al aan de orde is geweest in een traditioneel arbeidsrechtelijk geschil, in het meest waarschijnlijke geval een arbeidsrechtelijke klacht of een verzoek om arbitrage, dan wel een klacht inzake oneerlijke arbeidspraktijken bij de National Labor Relations Board. Dit doet zich bijvoorbeeld voor wanneer een werkgever in het kader van een collectieve

([10]) Zie http://www.ftc.gov/ftc/complaint.htm voor het on-lineklachtenformulier van de Federal Trade Commission.

([11]) Bijvoorbeeld in een recente zaak betreffende een piramideconstructie op internet waarbij de FTC het gedaan kreeg dat 15 622 consumenten uit de Verenigde Staten en uit 70 andere landen in totaal ongeveer 5,5 miljoen USD terugkregen. Zie www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftcrefund01.htm.

([12]) Tenzij dit specifiek is uitgesloten bij de wettelijke bevoegdheden van de FTC is haar jurisdictie in het kader van de FTC Act ten aanzien van handelspraktijken van dezelfde omvang als de constitutionele bevoegdheden van het Congres in het kader van de Commerce Clause, United States v. American Building Maintenance Industries, 422 U.S. 271, 277 n. 6 (1975). De bevoegdheid van de FTC strekt zich dus uit tot praktijken op personeelsgebied van bedrijven en industrieën in de internationale handel.

([13]) Zie „Online Auction Site Settles FTC Privacy Charges", persbericht van de FTC van 6 januari 2000, beschikbaar op http://www.ftc.gov/opa/2000/01/reverse4.htm.

arbeidsovereenkomst een verplichting ten aanzien van het gebruik van persoonsgegevens is aangegaan en de werknemer of de vakbond beweert dat de werkgever deze overeenkomst heeft geschonden. De FTC zal zich waarschijnlijk voegen naar die procedure ([14]).

Jurisdictie ten aanzien van keurmerkprogramma's

Ten tweede vroeg u de FTC of zij bevoegd is voor keurmerkprogramma's met mechanismen voor de oplossing van geschillen in de Verenigde Staten die een verkeerde voorstelling van zaken geven ten aanzien van hun rol bij de handhaving van de Veiligehavenbeginselen en de afhandeling van individuele klachten, ook indien dergelijke instanties technisch gezien niet winstgevend zijn. Om vast te stellen of de FTC bevoegd is voor een instantie die zegt geen winst na te streven, gaat zij zorgvuldig na of deze wellicht niet voor zichzelf winst wil maken, maar wel voor haar leden. De FTC heeft met succes staande gehouden jurisdictie over dergelijke instanties te hebben en op 24 mei 1999 heeft het Hooggerechtshof van de Verenigde Staten in de antitrustzaak, California Dental Association v. Federal Trade Commission, unaniem bevestigd dat de FTC jurisdictie heeft over een vereniging op vrijwillige basis zonder winstoogmerk van lokale vennootschappen van tandartsen. Het Hof bepaalde:

> Het is de bedoeling van de FTC Act dat deze niet alleen betrekking heeft op instanties die zijn opgezet om zaken te doen voor eigen profijt (titel 15 van de U.S.C., sectie 44), maar ook op instanties die zaken doen ten behoeve van haar leden. … Men kan er immers nauwelijks van uitgaan dat het Congres de bedoeling had het begrip ondersteunende organisaties dermate te beperken dat dit de gelegenheid zou bieden jurisdictie te vermijden terwijl het gezien de doelstellingen van de FTC Act juist wenselijk is dat dergelijke organisaties er wel onder vallen.

Kortom, om vast te stellen of de FTC bevoegd is voor een niet-winstgevende instantie die een keurmerkprogramma beheert, moet zij in concreto nagaan of de instantie economisch voordeel voor haar winstmakende leden biedt. Indien een dergelijke instantie een keurmerkprogramma exploiteert op een wijze die haar leden economisch voordeel biedt, is de FTC waarschijnlijk bevoegd. Afgezien daarvan is de FTC waarschijnlijk bevoegd voor een frauduleus keurmerkprogramma dat zich voordoet als een niet-winstgevende instantie.

Bescherming van de persoonlijke levenssfeer in een off-lineomgeving

Ten derde merkt u op dat onze eerdere correspondentie gericht was op de bescherming van de persoonlijke levenssfeer in een on-lineomgeving. Weliswaar is dit voor de FTC van groot belang omdat het een essentieel element voor de ontwikkeling van de elektronische handel is, maar de FTC Act dateert van 1914 en is dus ook van toepassing op een off-lineomgeving. We kunnen dus ook een zaak openen tegen off-linebedrijven die ten aanzien van de bescherming van de persoonlijke levenssfeer van de consumenten oneerlijke of misleidende handelspraktijken toepassen ([15]). In een in het afgelopen jaar door de FTC aanhangig gemaakte zaak, FTC v. TouchTone Information, Inc. ([16]), werd een informatiemakelaar ervan beschuldigd illegaal financiële informatie van consumenten te hebben gekregen en verkocht. De FTC beweerde dat TouchTone de informatie over de consumenten had verkregen door „voorwendselen" (pretexting), een term uit de detectivewereld ter beschrijving van de praktijk om informatie over andere personen te verzamelen door zich, meestal via de telefoon, anders voor te doen dan men in werkelijkheid is. In de zaak, die op 21 april 1999 in een federaal hof in Colorado werd geregistreerd, wordt gevraagd om een gerechtelijk bevel en om teruggave van alle illegaal gemaakte winsten.

Deze ervaring op het gebied van de rechtshandhaving, alsmede zorgen die de laatste tijd ontstaan over de samenvoeging van on-line- en off-linegegevensbanken, het vervagen van het onderscheid tussen on-line- en off-linehandelaren en het feit dat grote hoeveelheden persoonlijke informatie off line wordt verzameld en gebruikt, maken duidelijk dat veel aandacht moet worden besteed aan kwesties betreffende de bescherming van de persoonlijke levenssfeer in een off-lineomgeving.

Overlappende jurisdictie

Ten slotte stelt u een vraag over de wisselwerking tussen de jurisdictie van de FTC en die van andere met de rechtshandhaving belaste instanties, met name in gevallen waarin de jurisdicties van beide elkaar kunnen overlappen. De FTC

([14]) De vaststelling of er bij een bepaald gedrag sprake is van „oneerlijke arbeidspraktijken" of van een schending van een collectieve arbeidsovereenkomst is een technische kwestie, die gewoonlijk is voorbehouden aan de bevoegde arbeidsrechtbanken die dergelijke klachten behandelen, zoals arbiters en de NRLB.

([15]) Zoals u weet geeft de Fair Credit Reporting Act de FTC ook de bevoegdheid binnen het kader van de wet de persoonlijke levenssfeer van de consumenten op financieel gebied te beschermen; onlangs nog heeft de FTC een beslissing terzake genomen. Zie In the Matter of Trans Union, Docket No. 9255 (1 maart 2000) (persbericht en advies beschikbaar op www.ftc.gov/os/2000/03/index.htm#1).

([16]) Civil Action 99-WM-783 (D.Colo.) (beschikbaar op http://www.ftc.gov/opa/1999/9904/touchtone.htm) (hangende een voorlopig vonnis).

werkt nauw samen met tal van andere met de rechtshandhaving belaste instanties, waaronder de federale bankinstanties en de procureurs-generaal van de deelstaten. Zeer vaak coördineren we onze onderzoeken om maximaal profijt te hebben van onze middelen in gevallen waarin de jurisdictie elkaar overlapt. Ook verwijzen we zaken vaak voor onderzoek naar de juiste federale of deelstaatinstantie.

Ik hoop dat dit overzicht voor u van nut is. Voor nadere informatie kunt u zich altijd tot mij wenden.

Hoogachtend,

Robert Pitofsky

BIJLAGE VI

John Mogg
Directeur-generaal DG Markt
Europese Commissie
Kamer C 107-6/72
Wetstraat 200
B-1049 Brussel

Geachte heer Mogg,

Ik stuur u deze brief op verzoek van het ministerie van Handel van de Verenigde Staten om de rol van het ministerie van Vervoer bij de bescherming van de persoonlijke levenssfeer van consumenten met betrekking tot door hen aan luchtvaartmaatschappijen verstrekte gegevens uit te leggen.

Het ministerie van Vervoer stimuleert zelfregulering, omdat dit de eenvoudigste en efficiëntste manier is om de persoonlijke levenssfeer van de klanten bij de verwerking van door hen aan luchtvaartmaatschappijen verstrekte informatie te waarborgen. Het steunt dan ook de invoering van een veiligehavenregeling die luchtvaartmaatschappijen de mogelijkheid biedt om bij de doorgifte van informatie naar een niet-EU-land aan de eisen van de privacyrichtlijn van de Europese Unie te voldoen. Het ministerie erkent evenwel dat zelfregulering alleen effectief is wanneer luchtvaartmaatschappijen die zich verplichten de privacybeginselen van de veiligehavenregeling toe te passen, zich er ook aan houden. Daarom moet zelfregulering kracht worden bijgezet door juridische dwangmiddelen en zal het ministerie er op grond van zijn wettelijke taak de consumenten te beschermen voor zorgen dat luchtvaartmaatschappijen zich houden aan hun publieke privacybeloften, en zal het klachten die het van zelfregulerende organisaties en anderen, waaronder de lidstaten van de Europese Unie, over het niet nakomen van deze verplichtingen ontvangt, in behandeling nemen.

De bevoegdheid van het ministerie om op dit gebied naleving af te dwingen is gebaseerd op 49 U.S.C. 41712, dat een luchtvaartmaatschappij verbiedt om bij de verkoop van luchtvervoer oneerlijke of misleidende praktijken aan te wenden of oneerlijke concurrentiemethoden toe te passen indien dat (waarschijnlijk) tot gevolg heeft dat de consument schade wordt toegevoegd. Sectie 41712 is geënt op sectie 5 van de Federal Trade Commission Act (15 U.S.C. 45). Luchtvaartmaatschappijen zijn evenwel krachtens 15 U.S.C. 45(a)(2) vrijgesteld van een regeling overeenkomstig sectie 5 door de Federal Trade Commission.

Mijn bureau onderzoekt zaken uit hoofde van 49 U.S.C. 41712 en stelt eventueel een vervolging in. (Zie bv. DOT (Department of Trade) Orders 99-11-5 van 9 november 1999; 99-8-23 van 26 augustus 1999; 99-6-1 van 1 juni 1999; 98-6-24 van 22 juni 1998; 98-6-21 van 19 juni 1998; 98-5-31 van 22 mei 1998; en 97-12-23 van 18 december 1997.) Dergelijke zaken worden aanhangig gemaakt naar aanleiding van eigen onderzoek dan wel op grond van officiële en niet-officiële klachten die we ontvangen van particulieren, reisagenten, luchtvaartmaatschappijen en de nationale en buitenlandse overheidsinstanties.

Ik wil erop wijzen dat het feit dat een luchtvaartmaatschappij de privacy van reizigers bij de verwerking van de van hen ontvangen informatie niet in acht neemt, op zich geen schending van sectie 41712 betekent. Zodra een luchtvaartmaatschappij evenwel officieel en publiekelijk toezegt zich aan de Veiligehavenbeginselen ter bescherming van de persoonlijke levenssfeer van de consumenten ten aanzien van door hen verstrekte informatie te zullen houden, kan het ministerie zijn wettelijke bevoegdheden uit hoofde van sectie 41712 toepassen om te zorgen voor naleving van deze beginselen. Wanneer een passagier informatie verstrekt aan een luchtvaartmaatschappij die heeft toegezegd de Veiligehavenbeginselen te zullen naleven en de luchtvaartmaatschappij doet dit niet, kan dit de consument schade berokkenen en een overtreding van sectie 41712 betekenen. Mijn bureau zal het onderzoek van iedere klacht dienaangaande en de vervolging van iedere zaak die op dergelijke activiteiten duidt, een hoge prioriteit toekennen. Wij stellen het ministerie van Handel ook in kennis van het resultaat van dergelijke zaken.

Overtredingen van sectie 41712 kunnen leiden tot een verbod van dergelijke activiteiten en, wanneer hieraan geen gehoor wordt gegeven, tot civielrechtelijke sancties. Hoewel wij particuliere klagers geen schadevergoeding of geldelijke genoegdoening kunnen toekennen, kunnen wij op grond van eigen onderzoek en van door het ministerie voorgelegde zaken wel schikkingen goedkeuren waarbij de consumenten geldelijk voordeel krijgen, hetzij in mindering op dan wel ter compensatie van een geldboete die anders zou moeten worden betaald. Wij hebben dit in het verleden zo gedaan en wanneer de omstandigheden dit rechtvaardigen, kunnen wij dit ook doen in het kader van de Veiligehavenbeginselen. Herhaalde overtredingen van sectie 41712 door een luchtvaartmaatschappij uit de Verenigde Staten zou ook vragen opwerpen ten aanzien van haar bereidheid zich aan haar verplichtingen te houden, wat in flagrante gevallen tot gevolg zou kunnen hebben dat deze luchtvaartmaatschappij niet langer geschikt wordt geacht als zodanig werkzaam te zijn en

haar vergunning zou kwijtraken. (Zie DOT Orders 93-6-34 van 23 juni 1993 en 93-6-11 van 9 juni 1993. Hoewel deze maatregel niet op sectie 41712 betrekking had, had het wel tot gevolg dat de vergunning van een luchtvaartmaatschappij werd ingetrokken wegens een compleet negeren van de bepalingen van de Federal Aviation Act, een bilaterale overeenkomst, en de regels en voorschriften van het ministerie.)

Ik hoop dat deze informatie van nut zal zijn. Voor nadere vragen en voor meer informatie kunt u zich altijd tot mij wenden.

Hoogachtend,

Samuel Podberesky

Assistant General Counsel for
Aviation Enforcement and Proceeding

BIJLAGE VII

Overeenkomstig artikel 1, lid 2, onder b), kunnen in de Verenigde Staten de volgende overheidsinstanties klachten onderzoeken en na oneerlijke en misleidende praktijken herstel en schadeloosstelling voor de natuurlijke personen, ongeacht hun land van woonplaats of nationaliteit, verkrijgen, indien de overeenkomstig de FAQ's ten uitvoer gelegde beginselen niet worden nagekomen:

1. de Federal Trade Commission,

2. het ministerie van Vervoer.

De Federal Trade Commission (FTC) handelt op grond van haar bevoegdheid ingevolge sectie 5 van de Federal Trade Commission Act. Overeenkomstig sectie 5 is de FTC niet bevoegd voor banken en spaarbanken, kredietinstellingen, algemene telecommunicatiemaatschappijen, algemene vervoermaatschappijen, luchtvaartmaatschappijen en de vee- en vleeshandel. Hoewel de verzekeringssector niet specifiek in de lijst van uitzonderingen in sectie 5 is opgenomen, zijn volgens de McCarran-Ferguson Act [1] de staten bevoegd voor de regulering van deze sector. De bepalingen van de FTC Act zijn echter van toepassing op de verzekeringssector voorzover deze niet door de wetgeving van een staat is gereguleerd. Ook heeft de FTC restbevoegdheid op het gebied van oneerlijke of misleidende praktijken van verzekeringsmaatschappijen bij activiteiten buiten de verzekeringssector.

Het ministerie van Vervoer handelt op grond van zijn bevoegdheid ingevolge titel 49 van de United States Code, sectie 41712. Het ministerie van Handel leidt zaken in op grond van zijn eigen onderzoeken en op grond van formele en informele klachten van natuurlijke personen, reisorganisaties en luchtvaartmaatschappijen en van overheidsinstanties uit de Verenigde Staten of uit andere landen.

[1] Titel 15 van de U.S.C., sectie 1011 e.v.