II

(Besluiten waarvan de publicatie niet voorwaarde is voor de toepassing)

COMMISSIE

BESCHIKKING VAN DE COMMISSIE

van 14 mei 2004

betreffende de passende bescherming van persoonsgegevens in het Passenger Name Record van vliegtuigpassagiers die aan het Bureau of Customs and Border Protection van de Verenigde Staten worden doorgegeven

(Kennisgeving geschied onder nummer C(2004) 1914)

(Voor de EER relevante tekst)

(2004/535/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 vóór de doorgifte wordt voldaan aan de wetgeving van de lidstaten ter uitvoering van de andere bepalingen van de richtlijn.

(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, waarbij in het bijzonder rekening moet worden gehouden met een aantal elementen die van belang zijn voor de doorgifte, welke in artikel 25, lid 2, van de richtlijn zijn opgenomen.

(4) In het luchtverkeer is het Passenger Name Record (PNR) een bestand met de reisgegevens van elke passagier dat alle informatie bevat die de boekende en de deelnemende luchtvaartmaatschappijen nodig hebben om reserveringen te kunnen verwerken en controleren. Voor de toepassing van deze beschikking wordt onder „passagier" en „passagiers" tevens bemanningsleden verstaan. Onder „boekende luchtvaartmaatschappij" wordt verstaan de luchtvaartmaatschappij waarbij de passagier zijn reservering heeft geboekt of waarbij bijkomende reserveringen zijn geboekt nadat de reis is begonnen. Onder „deelnemende luchtvaartmaatschappijen" wordt verstaan iedere luchtvaartmaatschappij waarbij de boekende luchtvaartmaatschappij om een plaats op een of meer van haar vluchten heeft verzocht.

(5) Het Bureau of Customs and Border Protection (CBP) van het Department of Homeland Security (DHS) van de Verenigde Staten verlangt van elke luchtvaartmaatschappij die passagiersvluchten van en naar de Verenigde Staten verricht, elektronische toegang tot het PNR, voorzover PNR-gegevens worden vergaard en in het geautomatiseerde boekingssysteem van de luchtvaartmaatschappij worden opgeslagen.

(6) De vereisten inzake de doorgifte van persoonsgegevens uit het PNR van vliegtuigpassagiers aan het CBP zijn gebaseerd op een wet die door de Verenigde Staten in november 2001 [2] is goedgekeurd, en op uitvoeringsvoorschriften [3] die krachtens die wet door het CBP zijn vastgesteld.

[1] PB L 281 van 23.11.1995, blz. 31. Richtlijn laatstelijk gewijzigd bij Verordening (EG) nr. 1882/2003 (PB L 284 van 31.10.2003, blz. 1).

[2] Titel 49, United States Code, sectie 44909(c)(3).

[3] Titel 19, Code of Federal Regulations, sectie 122.49b.

(7) De desbetreffende wetgeving van de Verenigde Staten heeft betrekking op een grotere veiligheid en op de voorwaarden waaronder personen het land mogen binnenkomen en verlaten, aangelegenheden waarover de Verenigde Staten binnen het eigen rechtsgebied autonoom besluiten kunnen nemen. De vastgestelde bepalingen zijn overigens niet in strijd met door de Verenigde Staten aangegane internationale verplichtingen. De Verenigde Staten zijn een democratisch land en een rechtsstaat met een lange traditie van burgerlijke vrijheden. De legitimiteit van de wetgevingsprocedures en de capaciteit en onafhankelijkheid van het gerechtelijk apparaat in de Verenigde Staten staan niet ter discussie. Daarnaast is ook de persvrijheid een sterke garantie tegen elk misbruik van de burgerlijke vrijheden.

(8) De Gemeenschap steunt de Verenigde Staten ten volle in de strijd tegen het terrorisme binnen de grenzen van het Gemeenschapsrecht. Het Gemeenschapsrecht maakt het mogelijk een noodzakelijk evenwicht tot stand te brengen tussen veiligheidsbelangen en belangen welke verband houden met de persoonlijke levenssfeer. Zo bepaalt bijvoorbeeld artikel 13 van Richtlijn 95/46/EG dat de lidstaten wettelijke maatregelen kunnen nemen om de reikwijdte van bepaalde voorschriften van die richtlijn te beperken, indien dit noodzakelijk is om redenen van nationale veiligheid, defensie, openbare veiligheid en met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.

(9) De bedoelde doorgifte van gegevens betreft specifieke voor de verwerking verantwoordelijke instanties, namelijk luchtvaartmaatschappijen die tussen de Gemeenschap en de Verenigde Staten vliegen, en slechts één ontvanger in de Verenigde Staten, te weten het CBP.

(10) Elke regeling die een wettelijk kader creëert voor de doorgifte van PNR-gegevens naar de Verenigde Staten, met name door middel van deze beschikking, moet een beperkte looptijd hebben. Er is een periode van drie en een half jaar overeengekomen. Tijdens deze periode kan de situatie ingrijpend veranderen en de Gemeenschap en de Verenigde Staten zijn het erover eens dat de regeling zal moeten worden herzien.

(11) Voor de verwerking door het CBP van de doorgegeven persoonsgegevens uit het PNR van vliegtuigpassagiers gelden de voorwaarden die zijn vastgesteld in de verbintenissen van het Bureau of Customs and Border Protection (CBP) van het Department of Homeland Security van 11 mei 2004, (hierna „de verbintenissen" genoemd) en in de interne wetgeving van de Verenigde Staten waarnaar in die verbintenissen wordt verwezen.

(12) Wat de interne wetgeving van de Verenigde Staten betreft, is de Freedom of Information Act (FOIA) in dit verband in zoverre van belang dat daarin de voorwaarden zijn vastgesteld waaronder het CBP verzoeken om openbaarmaking kan weigeren en aldus het vertrouwelijke karakter van het PNR kan garanderen. Deze wet regelt de openbaarmaking van het PNR aan de belanghebbende, wat nauw aansluit bij het recht van toegang van de betrokkene. De FOIA is zonder onderscheid van toepassing op onderdanen en niet-onderdanen van de Verenigde Staten.

(13) De verbintenissen zijn of worden, overeenkomstig punt 44 ervan, in de Verenigde Staten in wetten, verordeningen, richtsnoeren of andere wetsteksten opgenomen en zullen zodoende in verschillende mate rechtskracht krijgen. De verbintenissen zullen onder verantwoordelijkheid van het DHS volledig in het Federal Register worden gepubliceerd. Deze verbintenissen getuigen van een serieus en weloverwogen politiek engagement van het DHS en de naleving ervan zal door de Gemeenschap en de Verenigde Staten gezamenlijk worden geëvalueerd. Niet-naleving ervan kan eventueel worden gewraakt met wettelijke, bestuursrechtelijke en politieke middelen; bij voortdurende niet-naleving kan de werking van deze beschikking worden opgeschort.

(14) De normen die het CBP bij het verwerken van PNR-gegevens op basis van de VS-wetgeving en de verbintenissen zal hanteren, voldoen aan de vereiste grondbeginselen voor een passend beschermingsniveau voor natuurlijke personen.

(15) Wat het beginsel van de gebruiksbeperking betreft, zullen de passagiersgegevens uit het PNR die aan het CBP worden doorgegeven, voor een specifiek doel worden gebruikt en daarna alleen nog worden aangewend of medegedeeld voorzover dit niet onverenigbaar is met het doel van de doorgifte. Meer bepaald zullen PNR gegevens uitsluitend worden gebruikt ter voorkoming en bestrijding van terrorisme en aanverwante misdrijven, andere zware misdrijven, waaronder georganiseerde misdaad, die van grensoverschrijdende aard zijn, alsook het ontvluchten van een aanhoudingsbevel of arrestatie wegens die misdrijven.

(16) Wat het beginsel van gegevenskwaliteit en het evenredigheidsbeginsel betreft, die moeten worden gezien in het licht van de belangrijke redenen van openbaar belang waarom PNR-gegevens worden doorgegeven, geldt dat deze gegevens na doorgifte aan het CBP door deze dienst achteraf niet zullen worden gewijzigd. Maximaal 34 PNR-categorieën van gegevens zullen aan de VS-autoriteiten worden doorgegeven en deze zullen de Commissie raadplegen alvorens nieuwe vereisten toe te voegen. Aanvullende persoonsgegevens waarom als rechtstreeks gevolg van PNR-gegevens wordt verzocht, zullen uit andere bronnen dan de overheid alleen langs legale weg worden verkregen. Over het algemeen zullen de PNR-gegevens na een periode van maximaal drie jaar en zes maanden worden vernietigd, met uitzondering van gegevens die voor specifiek onderzoek zijn gebruikt of anderszins manueel zijn geraadpleegd.

(17) Wat het transparantiebeginsel betreft, zal het CBP de reizigers van het doel van de doorgifte en verwerking van de gegevens en van de identiteit van de voor de verwerking verantwoordelijke instantie in het derde land op de hoogte stellen en hun ook andere informatie verstrekken.

(18) Wat het beveiligingsbeginsel betreft, neemt het CBP technische en organisatorische beveiligingsmaatregelen die in verhouding staan tot de aan de verwerking van de gegevens inherente risico's.

(19) Het recht op toegang tot en rectificatie van de gegevens wordt erkend, in die zin dat de betrokkene een kopie van de PNR-gegevens kan aanvragen en onjuiste gegevens kan laten corrigeren. De uitzonderingen waarin is voorzien, zijn grotendeels vergelijkbaar met de beperkingen die door de lidstaten overeenkomstig artikel 13 van Richtlijn 95/46/EG kunnen worden opgelegd.

(20) Verdere doorgifte naar andere overheidsinstanties, inclusief buitenlandse overheidsinstanties, met taken op het gebied van terrorismebestrijding of wetshandhaving geschiedt alleen per geval, voor doeleinden die in de verklaring over de beperking van de gebruiksdoeleinden zijn aangegeven. Doorgifte kan ook plaatsvinden ter bescherming van een vitaal belang van de betrokkene of van andere personen, meer bepaald wat betreft belangrijke gezondheidsrisico's, of bij strafrechtelijke vervolging van misdrijven, of in andere bij wet vastgestelde gevallen. Deze instanties zijn expliciet gebonden door de voorwaarden voor openbaarmaking; zij mogen de gegevens alleen voor het beoogde doel gebruiken en geen gegevens verder doorgeven zonder toestemming van het CBP. Andere buitenlandse, federale, staats-, of lokale instanties dan het CBP hebben geen rechtstreekse elektronische toegang tot de PNR-gegevens via de CPB-gegevensbanken. De openbaarmaking van PNR-gegevens zal door het CBP worden geweigerd op grond van ontheffingen van de desbetreffende bepalingen van de FOIA.

(21) Het CBP maakt geen gebruik van gevoelige gegevens in de zin van artikel 8 van Richtlijn 95/46/EG en verbindt zich ertoe, zolang er geen filtreersysteem bestaat om de doorgifte van dergelijke gegevens uit het PNR naar de Verenigde Staten te beletten, maatregelen te nemen om deze gegevens te vernietigen en, zolang dit niet gebeurd is, er geen gebruik van te maken.

(22) Wat betreft de handhavingsmechanismen om de naleving van deze beginselen door het CBP te waarborgen, is voorzien in opleiding en voorlichting van het personeel van deze dienst, alsook in de mogelijkheid om individuele personeelsleden te bestraffen. Op de eerbiediging van de privacy door het CPB in het algemeen wordt toegezien door de Chief Privacy Officer van het DHS, die ambtenaar is van het DHS, maar over een ruime organisatorische autonomie beschikt en jaarlijks verslag moet uitbrengen aan het Congres. Personen van wie PNR-gegevens zijn doorgegeven, kunnen bij het CPB, of, als dat niets oplevert, bij de Chief Privacy Officer van het DHS een klacht indienen, hetzij rechtstreeks, hetzij via de gegevensbeschermingsautoriteiten in de lidstaten. Klachten die door de gegevensbeschermingsautoriteiten van de lidstaten aan het DHS Privacy Office worden voorgelegd namens ingezetenen van de Gemeenschap die ontevreden zijn over de afhandeling van de klacht door het CBP of het DHS Privacy Office, worden onverwijld door het Privacy Office behandeld. De naleving van de verbintenissen zal elk jaar door het CBP in samenwerking met het DHS, en een team onder leiding van de Commissie gemeenschappelijk worden geëvalueerd.

(23) In het belang van de transparantie en om de bevoegde autoriteiten in de lidstaten in staat te stellen de bescherming van personen in verband met de verwerking van hun persoonsgegevens te waarborgen, is het noodzakelijk nader te regelen welke uitzonderlijke omstandigheden tot een opschorting van de doorgifte van gegevens kunnen leiden, ook al is er een passend beschermingsniveau vastgesteld.

(24) De bij artikel 29 van Richtlijn 95/46/EG ingestelde Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens heeft adviezen gegeven over het beschermingsniveau dat door de VS-autoriteiten voor passagiersgegevens wordt geboden, welke voor de Commissie als leidraad hebben gediend tijdens haar onderhandelingen met de DHS. De Commissie heeft nota genomen van deze adviezen [1].

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

HEEFT DE VOLGENDE BESCHIKKING GEGEVEN:

Artikel 1

Voor de toepassing van artikel 25, lid 2, van Richtlijn 95/46/EG wordt het Bureau of Customs and Border Protection van de Verenigde Staten, hierna „CBP" genoemd, geacht een passend beschermingsniveau te bieden voor PNR-gegevens die vanuit de Gemeenschap met betrekking tot vluchten van en naar de Verenigde Staten overeenkomstig de verbintenissen in de bijlage worden doorgegeven.

Artikel 2

Deze beschikking betreft het passende karakter van de bescherming die door het CBP wordt geboden om aan de vereisten van artikel 25, lid 1, van Richtlijn 95/46/EG te voldoen en laat andere voorwaarden of beperkingen tot uitvoering van andere bepalingen van die richtlijn die op de verwerking van persoonsgegevens in de lidstaten betrekking hebben, onverlet.

[1] Advies 6/2002 over de doorgifte van informatie van de passagierslijst en andere gegevens van luchtvaartmaatschappijen aan de Verenigde Staten, goedgekeurd door de Groep op 24 oktober 2002, beschikbaar op het volgende adres:
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp66_en.pdf
Advies 4/2003 over het in de Verenigde Staten voor de doorgifte van passagiersgegevens gewaarborgde beschermingsniveau, goedgekeurd door de Groep op 13 juni 2003, beschikbaar op het volgende adres:
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf
Advies 2/2004 over de passende bescherming van in het PNR van passagiers vervatte persoonsgegevens die aan het Bureau of Customs and Border Protection van de Verenigde Staten (CBP) worden doorgegeven, goedgekeurd door de Groep op 29 januari 2004,, beschikbaar op het volgende adres:
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp87_en.pdf

Artikel 3

1. Onverminderd hun bevoegdheden om stappen te ondernemen ter naleving van nationale bepalingen die zijn vastgesteld ingevolge andere bepalingen dan artikel 25 van Richtlijn 95/46/EG, kunnen de bevoegde autoriteiten in de lidstaten gebruikmaken van hun bestaande bevoegdheden om de overdracht van gegevens aan het CBP op te schorten, teneinde personen bij de verwerking van hun persoonsgegevens te beschermen in de volgende gevallen:

a) wanneer een bevoegde VS-autoriteit heeft vastgesteld dat het CBP in strijd met de toepasselijke normen voor gegevensbescherming handelt, of

b) wanneer het zeer waarschijnlijk is dat niet aan de in de bijlage vastgestelde normen voor gegevensbescherming wordt voldaan, er gegronde redenen zijn om aan te nemen dat het CBP niet tijdig passende maatregelen neemt of zal nemen om het desbetreffende probleem op te lossen, de voortzetting van de doorgifte een dreigend gevaar voor ernstige schade voor de betrokkene inhoudt en de bevoegde autoriteiten in de lidstaat naar de omstandigheden in redelijkheid inspanningen hebben geleverd om het CBP in kennis te stellen en de gelegenheid te geven te reageren.

2. De opschorting eindigt zodra is gewaarborgd dat de beschermingsnormen worden nageleefd en de bevoegde autoriteiten van de betrokken lidstaten hiervan in kennis zijn gesteld.

Artikel 4

1. De lidstaten stellen de Commissie onverwijld in kennis wanneer op grond van artikel 3 maatregelen worden genomen.

2. De lidstaten en de Commissie stellen elkaar in kennis van iedere wijziging in de normen voor gegevensbescherming en van de gevallen waarin de instanties die verantwoordelijk zijn voor de naleving door het CBP van de in de bijlage vastgestelde beschermingsnormen verzuimen deze naleving te garanderen.

3. Wanneer uit de overeenkomstig artikel 3 en de leden 1 en 2 van dit artikel verzamelde informatie mocht blijken dat niet langer aan de vereiste grondbeginselen voor een passend beschermingsniveau voor natuurlijke personen wordt voldaan, of dat een instantie die verantwoordelijk is voor de naleving door het CBP van de in de bijlage vastgestelde beschermingsnormen haar taak niet naar behoren vervult, wordt het CBP hiervan in kennis gesteld en wordt, indien nodig, de in artikel 31, lid 2, van Richtlijn 95/46/EG bedoelde procedure toegepast om deze beschikking in te trekken of op te schorten.

Artikel 5

De werking van deze beschikking wordt geëvalueerd en alle relevante bevindingen worden medegedeeld aan het bij artikel 31 van Richtlijn 95/46/EG ingestelde comité, met inbegrip van ieder bewijs dat van invloed kan zijn op de in artikel 1 van deze beschikking vervatte vaststelling dat de bescherming van in het PNR van vliegtuigpassagiers voorkomende persoonsgegevens die aan het CBP worden doorgegeven, passend is in de zin van artikel 25 van Richtlijn 95/46/EG.

Artikel 6

De lidstaten nemen alle noodzakelijke maatregelen om binnen vier maanden na kennisgeving van deze beschikking aan deze beschikking te voldoen.

Artikel 7

Deze beschikking komt drie jaar en zes maanden na de datum van kennisgeving ervan te vervallen, tenzij zij overeenkomstig de in artikel 31, lid 2, van Richtlijn 95/46/EG bedoelde procedure wordt verlengd.

Artikel 8

Deze beschikking is gericht tot de lidstaten.

Gedaan te Brussel, 14 mei 2004.

Voor de Commissie
Frederik BOLKESTEIN
Lid van de Commissie

BIJLAGE

VERBINTENISSEN VAN HET BUREAU OF CUSTOMS AND BORDER PROTECTION (CBP) VAN HET DEPARTMENT OF HOMELAND SECURITY

Ter ondersteuning van het voornemen van de Europese Commissie (hierna „de Commissie" genoemd) om de haar bij artikel 25, lid 6, van Richtlijn 95/46/EG (hierna „de richtlijn" genoemd) verleende bevoegdheden uit te oefenen en een besluit vast te stellen waarbij wordt erkend dat het Bureau of Customs and Border Protection (CBP) van het Department of Homeland Security een passende bescherming biedt voor de doorgifte door luchtvaartmaatschappijen van PNR-gegevens (Passenger [1] Name Record) die binnen het toepassingsgebied van de richtlijn kunnen vallen, gaat het CBP de volgende verbintenissen aan.

Wettelijke bevoegdheid om PNR-gegevens te verkrijgen

1. Bij wet (titel 49, United States Code, sectie 44909(c)(3)) en de (voorlopige) regelgeving tot uitvoering ervan (titel 19, Code of Federal Regulations, sectie 122.49b), zijn alle luchtvaartmaatschappijen die passagiersvluchten in het buitenlandse luchtvervoer naar of uit de Verenigde Staten verrichten, verplicht het CBP (voorheen: US Customs Service) elektronische toegang tot PNR-gegevens te verschaffen, voorzover deze zijn verzameld en in hun geautomatiseerde boekings- en vertrekcontrolesystemen („boekingssystemen") zijn opgeslagen.

Gebruik van PNR-gegevens door het CBP

2. De meeste gegevenselementen in het PNR kunnen door het CBP worden verkregen door uit hoofde van zijn normale grenscontrolebevoegdheid het vliegbiljet en andere reisdocumenten van de betrokkene te onderzoeken, maar de mogelijkheid om deze gegevens in elektronische vorm te ontvangen, zal het potentieel van het CBP om het bonafide reizen te vergemakkelijken en efficiënte voorafgaande risicobeoordelingen van passagiers te verrichten, aanzienlijk vergroten.

3. PNR-gegevens worden door het CBP uitsluitend gebruikt ter preventie en bestrijding van: 1. terrorisme en aanverwante vormen van criminaliteit; 2. andere zware misdrijven, waaronder georganiseerde misdaad, die van transnationale aard zijn, en 3. ontvluchten van aanhoudingsbevelen of arrestatie voor de bovengenoemde misdrijven. Door daarvoor PNR-gegevens te gebruiken, kan het CBP zijn middelen concentreren op aangelegenheden met hoog risico, zodat het bonafide reizen gemakkelijker en veiliger wordt.

Vereiste gegevens

4. De door het CBP vereiste gegevenselementen (hierna „PNR" genoemd) worden in aanhangsel A opgesomd. Hoewel het CBP toegang verlangt tot elk van de vierendertig (34) gegevenselementen van de lijst in aanhangsel A, meent het dat een individueel PNR zelden al die gegevens zal bevatten. Wanneer het PNR niet al die gegevens bevat, zal het CBP via het boekingssysteem van de luchtvaartmaatschappij geen directe toegang trachten te krijgen tot andere PNR-gegevens die niet op de lijst in aanhangsel A staan.

5. Wat de met „OSI" en „SSI/SSR" aangeduide gegevenselementen betreft (meestal algemene opmerkingen en open velden), zal het geautomatiseerde systeem van het CBP die velden voor alle andere in aanhangsel A opgesomde gegevenselementen doorzoeken. Het CBP-personeel zal niet gemachtigd zijn om de volledige OSI- en SSI/SSR-velden manueel te doorzoeken, tenzij de persoon op wie het PNR betrekking heeft, door het CBP is geïdentificeerd als een hoog risico in verband met een van de in punt 3 vermelde doeleinden.

6. Aanvullende persoonsgegevens die als rechtstreeks gevolg van PNR-gegevens worden gevraagd, zullen van andere bronnen dan de overheid uitsluitend langs legale weg worden verkregen, onder meer door in voorkomend geval gebruik te maken van de gebruikelijke wederzijdse rechtsbijstand, en alleen voor de in overweging 3 genoemde doeleinden. Als bijvoorbeeld een creditcardnummer in een PNR is opgenomen, kan informatie over transacties met betrekking tot die rekening worden opgevraagd in het kader van een wettelijke procedure, zoals bijvoorbeeld een dagvaarding door een „grand jury" of een rechterlijke beslissing, of in andere gevallen waarin de wet voorziet. Voorts zal de toegang tot bestanden in verband met e-mailrekeningen op basis van een PNR worden geregeld krachtens de wettelijke bepalingen van de Verenigde Staten voor dagvaardingen, rechterlijke beslissingen, aanhoudingsbevelen en andere procedures waarin de wet voorziet, al naar gelang de gewenste soort informatie.

7. Het CBP zal met de Europese Commissie van tevoren overleg plegen over een eventuele herziening van de verlangde PNR-gegevenselementen (aanhangsel A), indien het van oordeel is dat de luchtvaartmaatschappijen extra PNR-velden aan hun systemen zouden kunnen toevoegen om de capaciteit van het CBP tot het verrichten van risicobeoordelingen van passagiers aanzienlijk te vergroten, of als mocht blijken dat een eerder niet verlangd PNR-veld nodig zal zijn om de beperkte in punt 3 van deze verbintenissen beoogde doelstellingen te verwezenlijken.

[1] In deze verbintenissen wordt onder „passagier" en „passagiers" tevens bemanningsleden verstaan.

8. Het CBP kan PNR's „en bloc" aan de Transportation Security Administration (TSA) doorgeven om deze op haar computerondersteunde passagiersdoorlichtingssysteem (Computer Assisted Passenger Prescreening System II, CAPPS II) te testen. Een dergelijke doorgifte vindt pas plaats nadat toestemming is verkregen om de PNR-gegevens van Amerikaanse binnenlandse vluchten te testen. Overeenkomstig deze bepaling doorgegeven PNR-gegevens zullen door de TSA of door andere, direct bij de tests betrokken partijen niet langer worden bewaard dan de voor de tests vereiste termijn en zullen ook niet aan derden worden doorgegeven ([2]). De verwerking van de gegevens heeft uitsluitend ten doel het CAPPS II en de interfaces te testen en mag geen operationele gevolgen hebben, behoudens in noodsituaties wanneer een bekende terrorist of een persoon van wie bekend is dat hij banden met het terrorisme heeft, wordt geïdentificeerd. Krachtens de bepaling die een automatische filtreermethode vereist, zoals beschreven in punt 10, zal het CBP „gevoelige" gegevens filtreren en wissen voordat PNR's volgens dit punt „en bloc" aan de TSA worden doorgegeven.

Behandeling van „gevoelige" gegevens

9. Het CBP zal geen „gevoelige" gegevens (d.w.z. persoonlijke gegevens waaruit het ras of de etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, en gegevens die de gezondheid of het seksuele leven betreffen) uit het PNR gebruiken, zoals hieronder wordt beschreven.

10. Het CBP zal op zo kort mogelijke termijn een geautomatiseerd systeem opzetten dat bepaalde, in overleg met de Europese Commissie vastgestelde „gevoelige" PNR-codes en -termen filtreert en wist.

11. Zolang dergelijke automatische filters niet kunnen worden toegepast, verklaart het CBP dat het geen „gevoelige" PNR-gegevens gebruikt of zal gebruiken en verbindt zich ertoe dergelijke gegevens in geval van discretionaire openbaarmaking van PNR overeenkomstig de punten 28 tot en met 34 te wissen ([3]).

Wijze van toegang tot PNR-gegevens

12. Wat de PNR-gegevens betreft waartoe het CBP via de boekingssystemen van de luchtvaartmaatschappijen direct toegang heeft (of krijgt) om personen te identificeren die voor grenscontrole in aanmerking kunnen komen, zal het personeel van het CBP alleen toegang hebben (of krijgen) en gebruikmaken van PNR-gegevens van personen van wie de reis een vlucht naar of vanuit ([4]) de Verenigde Staten omvat.

13. Het CBP zal passagiersgegevens uit boekingssystemen van luchtvaartmaatschappijen „ophalen" totdat de luchtvaartmaatschappijen in staat zijn een systeem toe te passen om de gegevens zelf aan het CBP „toe te leveren".

14. Het CBP zal PNR-gegevens in verband met een specifieke vlucht niet eerder dan 72 uur vóór het vertrek van die vlucht ophalen en zal de boekingssystemen tussen de eerste ophaling van die gegevens, het vertrek van de vlucht uit het buitenland en de aankomst van de vlucht in de Verenigde Staten, of tussen de eerste ophaling van die gegevens en het vertrek van de vlucht vanuit de Verenigde Staten hoogstens driemaal (3) opnieuw controleren om na te gaan of de informatie al dan niet is gewijzigd. Indien de luchtvaartmaatschappijen over de mogelijkheid beschikken PNR-gegevens „toe te leveren", dient het CBP deze 72 uur vóór het vertrek van de vlucht te ontvangen, op voorwaarde dat alle wijzigingen die tussen dat tijdstip en de tijd van aankomst in of vertrek uit de Verenigde Staten in de PNR-gegevens worden aangebracht, eveneens aan het CBP worden toegeleverd ([5]). In het uitzonderlijke geval dat het CBP van tevoren informatie ontvangt dat een of meer personen die bijzondere aandacht verdienen, misschien een vlucht naar, vanuit of via de Verenigde Staten gaan nemen, kan het CBP meer dan 72 uur vóór het vertrek van de vlucht PNR-gegevens ophalen (of om speciale toelevering ervan verzoeken) opdat passende maatregelen kunnen worden genomen wanneer deze essentieel zijn om een van de in punt 3 genoemde misdrijven te voorkomen of te bestrijden. In gevallen waarin het CBP inderdaad meer dan 72 uur vóór het vertrek van de vlucht toegang moet hebben tot PNR-gegevens, zal het in de mate van het mogelijke de gebruikelijke wetshandhavingskanalen volgen.

([2]) Voor de toepassing van deze bepaling wordt het CBP niet als een direct bij de CAPPS II-tests betrokken partij of als „derde" beschouwd.
([3]) Indien, voordat het CBP automatische filters gaat toepassen (zoals bedoeld in punt 10), „gevoelige" gegevens voorkomen in een PNR dat op niet discretionaire wijze openbaar wordt gemaakt zoals beschreven in punt 35, zal het CBP zijn uiterste best doen om de openbaarmaking van „gevoelige" PNR-gegevens overeenkomstig de VS-wetgeving te beperken.
([4]) Dit geldt ook voor personen die op doorreis zijn in de Verenigde Staten.
([5]) Indien de luchtvaartmaatschappijen bereid zijn de PNR-gegevens aan het CBP toe te leveren, zal het CBP met de luchtvaartmaatschappijen de mogelijkheid bespreken om op gezette tijden tussen 72 uur vóór het vertrek van de vlucht uit het buitenland en de aankomst van de vlucht in de Verenigde Staten of binnen 72 uur vóór het vertrek van de vlucht uit de Verenigde Staten, al naar gelang het geval, PNR-gegevens toe te leveren. Het CBP geeft de voorkeur aan een methode waarmee de voor effectieve risicobeoordeling vereiste PNR-gegevens worden toegeleverd, terwijl het economische effect ervan op de luchtvaartmaatschappijen zoveel mogelijk wordt beperkt.

Opslag van PNR-gegevens

15. Behoudens goedkeuring door de National Archives and Records Administration (44 United States Code 2101, e.v.), zal het CBP de on-linetoegang tot PNR-gegevens gedurende een periode van zeven (7) dagen tot geautoriseerde CBP-gebruikers ([6]) beperken, waarna het aantal functionarissen die gemachtigd zijn om toegang te krijgen tot PNR-gegevens, nog verder zal worden beperkt gedurende een periode van drie jaar en zes maanden (3,5 jaar), gerekend vanaf de datum waarop het CBP toegang kreeg tot de gegevens uit het boekingssysteem van de luchtvaartmaatschappij (of deze gegevens ontving). Na drieëneenhalf jaar zullen PNR-gegevens waartoe geen manuele toegang heeft plaatsgevonden, worden vernietigd. PNR-gegevens die in de eerste drieëneenhalf jaar manueel zijn geraadpleegd, zullen door het CBP worden overgedragen naar een bestand met gewiste dossiers ([7]), waarin zij acht (8) jaar opgeslagen blijven en dan worden vernietigd. Dit tijdschema zal echter niet gelden voor PNR-gegevens die verband houden met een specifiek onderzoeksdossier (dergelijke gegevens zullen toegankelijk blijven totdat het dossier is gearchiveerd). Voor PNR-gegevens waartoe het CBP via boekingssystemen van luchtvaartmaatschappijen directe toegang heeft (of die het CBP heeft ontvangen) tijdens de feitelijke duur van deze verbintenissen, zal het CBP de in dit punt geschetste opslagbeleid volgen, ook al bestaat de mogelijkheid dat de in punt 46 aangegane verbintenissen komen te vervallen.

Beveiliging van het computersysteem van het CBP

16. Geautoriseerd CBP-personeel krijgt toegang tot PNR via het gesloten CBP-intranetsysteem dat compleet gecodeerd is en de verbinding wordt door het Customs Data Center beheerd. De in de databank van het CBP opgeslagen PNR-gegevens zijn alleen „read only"-toegankelijk voor daartoe gemachtigde personeelsleden, d.w.z. dat de meeste gegevens programmatisch kunnen worden geherformatteerd, maar dat zij door het CBP op geen enkele wijze substantieel zullen worden gewijzigd zodra het CBP via het boekingssysteem van een luchtvaartmaatschappij toegang daartoe heeft gekregen.

17. Geen andere buitenlandse, federale, staats- of lokale instantie heeft directe elektronische toegang tot PNR-gegevens via databanken van het CBP (of via het Interagency Border Inspection System (IBIS)).

18. Nadere bijzonderheden over de toegang tot informatie in CBP-databanken (zoals wie, waar, wanneer (datum en uur) en alle herzieningen van de gegevens) worden automatisch geregistreerd en routinematig gecontroleerd door het Office of Internal Affairs om onrechtmatig gebruik van het systeem te voorkomen.

19. Alleen bepaalde CBP-functionarissen, -werknemers en IT-contractanten ([8]) (onder toezicht van het CBP) die met goed gevolg een antecedentenonderzoek hebben ondergaan, die een actieve, met een password beveiligde „boekhouding" (account) in het computersysteem van het CBP hebben en die officieel bevoegd zijn verklaard om PNR-gegevens te onderzoeken, krijgen toegang tot die gegevens.

20. CBP-functionarissen, -werknemers en -contractanten zijn verplicht om de twee jaar een opleiding in beveiliging en gegevensbescherming te volgen en te slagen in een test. CBP-systeemaudits worden verricht om de naleving van alle voorschriften inzake privacy en beveiliging van gegevens te verifiëren en te waarborgen.

21. Voor onrechtmatige toegang van CBP-personeel tot boekingssystemen van luchtvaartmaatschappijen of tot het CBP-computersysteem waarin PNR's zijn opgeslagen, gelden strenge tuchtmaatregelen (waaronder eventueel ontslag) en kunnen zelfs strafrechtelijke sancties worden opgelegd (boetes, gevangenisstraffen van maximaal één jaar of beide) (zie titel 18, United States Code, sectie 1030).

22. In haar beleidslijnen en voorschriften voorziet het CBP ook in strenge tuchtmaatregelen (waaronder eventeel ontslag) voor elke CBP-werknemer die zonder officiële machtiging informatie uit CBP-computersystemen openbaar maakt (titel 19, Code of Federal Regulations, sectie 103.34).

23. Strafrechtelijke sancties (zoals boetes, gevangenisstraffen van maximaal één jaar of beide) kunnen aan elke functionaris of werknemer van de Verenigde Staten worden opgelegd wegens openbaarmaking van tijdens de uitoefening van zijn functie verkregen PNR-gegevens, indien de openbaarmaking ervan wettelijk verboden is (zie titel 18, United States Code, secties 641, 1030 en 1905).

([6]) Onder geautoriseerde CBP-gebruikers wordt onder meer verstaan: werknemers bij analytische eenheden in de lokale kantoren, alsook werknemers in het National Targeting Center. Zoals reeds aangegeven, zullen de personen die met het onderhoud, de ontwikkeling en audits van de CBP-databank zijn belast, voor deze beperkte doeleinden eveneens toegang krijgen tot dergelijke gegevens.

([7]) Hoewel het PNR-document uit technisch oogpunt niet gewist is als het naar het bestand met gewiste documenten wordt overgedragen, wordt het als onbewerkte gegevens opgeslagen (geen makkelijk terug te zoeken formulier en vandaar onbruikbaar voor „traditioneel" onderzoek op het gebied van wetshandhaving) en is het alleen beschikbaar voor geautoriseerd personeel bij het Office of Internal Affairs van het CBP (en in sommige gevallen bij het Office of the Inspector General in verband met audits) en voor het personeel dat belast is met het onderhoud van de databank bij het Office of Information Technology van het CBP, en wel op basis van „need-to-know".

([8]) De toegang van „contractanten" tot PNR-gegevens in de CBP-computersystemen zou worden toevertrouwd aan personen die bij het CBP een contract hebben om te helpen bij het onderhoud of de ontwikkeling van zijn computersysteem.

Behandeling en bescherming van PNR-gegevens door het CBP

24. Het CBP behandelt PNR-informatie over personen, ongeacht hun nationaliteit of land van vestiging, als voor wetshandhaving gevoelige, vertrouwelijke persoonlijke informatie van de betrokkenen en als vertrouwelijke commerciële informatie van de luchtvaartmaatschappij en zal dergelijke gegevens derhalve niet openbaar maken, tenzij zulks in deze verbintenissen is bepaald of van rechtswege wordt geëist.

25. De openbaarmaking van PNR-gegevens valt in het algemeen onder de FOIA (titel 5, United States Code, sectie 552), waarbij iedereen (ongeacht zijn nationaliteit of land van vestiging) toegang krijgt tot de bestanden van een federale instantie van de Verenigde Staten, tenzij deze bestanden (of een deel ervan) door een krachtens de FOIA verleende ontheffing tegen openbaarmaking worden beschermd. Zo mag bijvoorbeeld een instantie de openbaarmaking van een bestand (of een deel ervan) weigeren, als het om vertrouwelijke commerciële informatie gaat, als de openbaarmaking van de informatie een duidelijke ongerechtvaardigde inbreuk op de persoonlijke levenssfeer zou vormen of als de informatie voor wetshandhavingsdoeleinden wordt verzameld, zodat de openbaarmaking ervan naar alle waarschijnlijkheid een ongerechtvaardigde inbreuk op de persoonlijke levenssfeer zal vormen (titel 5, United States Code, sectie 552(b)(4), (6), (7)(C)).

26. De CBP-voorschriften (titel 19, Code of Federal Regulations, sectie 103.12) met betrekking tot de behandeling van verzoeken om informatie (zoals PNR-gegevens) krachtens de FOIA, bepaalt met name dat (met een beperkt aantal uitzonderingen wanneer de betrokkene er zelf om verzoekt) de openbaarmakingsvoorschriften van de FOIA niet gelden voor CBP-bestanden met betrekking tot: 1. vertrouwelijke commerciële informatie; 2. materiaal in verband met de persoonlijke levenssfeer, waarvan de openbaarmaking een duidelijke ongerechtvaardigde inbreuk op de persoonlijke levenssfeer zou betekenen, en 3. informatie die voor wetshandhavingsdoeleinden is verzameld en waarvan de openbaarmaking naar alle waarschijnlijkheid een ongerechtvaardigde inbreuk op de persoonlijke levenssfeer zal vormen ([9]).

27. Wat administratieve of gerechtelijke procedures als gevolg van een krachtens de FOIA ingediend verzoek om PNR-informatie van luchtvaartmaatschappijen betreft, zal het CBP ervan uitgaan dat dergelijke bestanden niet onder de openbaarmakingsvoorschriften van de FOIA vallen.

Doorgifte van PNR-gegevens aan andere overheidsinstanties

28. Behalve voor de doorgifte tussen het CBP en de TSA overeenkomstig punt 8, zullen de diensten van het Department of Homeland Security (DHS) worden behandeld als „derden" waarvoor inzake de uitwisseling van PNR-gegevens dezelfde regels en voorwaarden gelden als voor andere overheidsdiensten dan het DHS.

29. Het CBP zal, naar eigen goeddunken, andere met terrorismebestrijding of wetshandhaving belaste overheidsinstanties, waaronder ook buitenlandse overheidsinstanties, alleen PNR-gegevens verstrekken, en zulks per geval, om misdrijven zoals bedoeld in punt 3 te voorkomen en te bestrijden. (De autoriteiten waarmee het CBP bereid is dergelijke gegevens uit te wisselen, worden hierna de „aangewezen autoriteiten" genoemd.)

30. Het CBP zal behoedzaam te werk gaan voordat het besluit PNR-gegevens voor de genoemde doeleinden door te geven. Het zal eerst nagaan of de aangevoerde reden om de PNR-gegevens naar een andere aangewezen instantie door te geven, strookt met de aangegeven doelstelling (zie punt 29). In voorkomend geval zal het CBP nagaan of die aangewezen autoriteit verantwoordelijk is voor preventie, onderzoek of vervolging van schendingen, dan wel voor handhaving of uitvoering van wet- of regelgeving met betrekking tot die doelstelling, voorzover het CBP vermoedt dat er sprake is van schending of potentiële schending van de wet. De voor- en nadelen van de openbaarmaking zullen met inachtneming van alle gegeven omstandigheden tegen elkaar moeten worden afgewogen.

31. Wat de regulering van de verspreiding van PNR-gegevens betreft die met andere aangewezen autoriteiten kunnen worden uitgewisseld, wordt het CBP beschouwd als „eigenaar" van de gegevens en zijn die aangewezen autoriteiten op grond van de uitdrukkelijke voorwaarden van openbaarmaking verplicht: 1. de PNR-gegevens alleen te gebruiken voor de in punt 29 of 34 aangegeven doeleinden; 2. te zorgen voor de behoorlijke opslag van de ontvangen PNR-informatie, zulks volgens de door de aangewezen autoriteit toegepaste procedures voor het bewaren van bestanden, en 3. de uitdrukkelijke toestemming van het CBP te krijgen voor elke verdere verspreiding. Niet-naleving van de voorwaarden voor doorgifte kan worden onderzocht en gerapporteerd door de Chief Privacy Officer van het DHS en kan tot gevolg hebben dat de aangewezen autoriteit niet meer in aanmerking komt om PNR-gegevens van het CBP te ontvangen.

([9]) Het CBP zou zich uniform op deze uitzonderingen beroepen, ongeacht de nationaliteit of het land van vestiging van de betrokkene.

32. Elke openbaarmaking van PNR-gegevens door het CBP vindt plaats onder de uitdrukkelijke voorwaarde dat de ontvanger deze gegevens behandelt als vertrouwelijke commerciële informatie en voor wetshandhaving gevoelige, vertrouwelijke persoonlijke informatie van de betrokkene, zoals bedoeld in de punten 25 en 26, waarvoor de verplichting tot openbaarmaking krachtens de Freedom of Information Act (5 USC 552) niet geldt. Voorts zal de ontvanger erop worden geattendeerd dat verdere openbaarmaking van dergelijke informatie niet is toegestaan zonder uitdrukkelijke voorafgaande toestemming van het CBP. Het CBP zal geen verdere doorgifte van PNR-gegevens toestaan voor andere doeleinden dan die van punt 29, 34 of 35.

33. Werknemers van dergelijke aangewezen autoriteiten, die zonder de vereiste toestemming PNR-gegevens openbaar maken, stellen zich bloot aan strafrechtelijke sancties (titel 18, United States Code, secties 641, 1030 en 1905).

34. Geen van de onderhavige bepalingen belet het gebruik van PNR-gegevens door of de openbaarmaking ervan aan relevante overheidsdiensten, voorzover die openbaarmaking noodzakelijk is om de essentiële belangen van de betrokkene of van andere personen te behartigen, vooral als het om significante gezondheidsrisico's gaat. Voor openbaarmaking voor deze doeleinden gelden dezelfde doorgiftevoorwaarden als in de punten 31 en 32 van deze verbintenissen.

35. Geen enkele bepaling in deze verbintenissen belet het gebruik of de openbaarmaking van PNR-gegevens bij strafrechtelijke procedures of in andere wettelijk voorgeschreven gevallen. Het CBP zal de Europese Commissie informeren over de goedkeuring van VS-wetgeving waardoor de verklaringen in deze verbintenissen substantieel worden beïnvloed.

Kennisgeving aan de betrokkenen, toegang van de betrokkenen tot PNR-gegevens en de hun geboden verhaalsmogelijkheden

36. Het CBP zal de reizigers informatie verstrekken over de eisen inzake PNR en de aan het gebruik ervan gerelateerde kwesties (algemene informatie over de bevoegheid op grond waarvan de gegevens worden verzameld, doel van de verzameling, gegevensbescherming, uitwisseling van gegevens, identiteit van de verantwoordelijke ambtenaar, beschikbare beroepsprocedures en contactadressen voor personen met vragen of problemen enz., om op de website van het CBP te plaatsen, in reisbrochures af te drukken enz.).

37. Verzoeken van de betrokkene (ook wel „verzoeker van de eerste partij" genoemd) om een kopie te ontvangen van de PNR-gegevens in de CBP-databanken met betrekking tot de betrokkene, worden behandeld overeenkomstig de FOIA. Dergelijke verzoeken kunnen worden gericht aan: Freedom of Information Act (FOIA) Request, US Customs and Border Protection, 1300 Pennsylvania Avenue, NW, Washington, DC 20229, indien zij per post worden ingediend; het verzoek kan ook worden ingediend bij de Disclosure Law Officer, US Customs and Border Protection, Headquarters, Washington, DC. Voor meer informatie over de procedures om FOIA-verzoeken in te dienen, wordt verwezen naar de US Code of Federal Regulations, sectie 103.5, titel 19. In geval van een verzoeker van de eerste partij zal het feit dat het CBP PNR-gegevens over het algemeen als vertrouwelijke persoonlijke informatie over de betrokkene en als vertrouwelijke commerciële informatie van de luchtvaartmaatschappij beschouwt, door het CBP niet worden aangevoerd als reden om de betrokkene overeenkomstig de FOIA PNR-gegevens te onthouden.

38. In bepaalde uitzonderlijke omstandigheden kan het CBP zich op de hem bij de FOIA verleende bevoegdheid beroepen om de openbaarmaking van het volledige PNR-bestand (of wellicht eerder een deel ervan) aan een verzoeker van de eerste partij krachtens titel 5, United States Code, sectie 552(b), te weigeren of uit te stellen (bv. indien door openbaarmaking overeenkomstig de FOIA „naar verwachting de onderzoeksprocedures zullen worden belemmerd" of „technieken en procedures voor wetshandhavingsonderzoek zouden worden onthuld ... [wat] wel eens tot wetsontduiking zou kunnen leiden"). Volgens de FOIA heeft elke verzoeker het recht om het besluit van het CBP tot het achterhouden van informatie administratief en gerechtelijk aan te vechten (zie 5 USC 552(a)(4)(B); 19 CFR 103.7-103.9).

39. Het CBP verbindt zich ertoe om op verzoek van passagiers en bemanningsleden, luchtvaartmaatschappijen of gegevensbeschermingsautoriteiten in de EU-lidstaten (voorzover zij daartoe door de betrokkene specifiek zijn gemachtigd) gegevens te rectificeren ([10]), indien het vaststelt dat die gegevens in zijn databank zijn opgeslagen en dat een correctie gerechtvaardigd is en naar behoren wordt gestaafd. Het CBP zal elke aangewezen autoriteit die dergelijke PNR-gegevens heeft ontvangen, van alle substantiële rectificaties van die gegevens in kennis stellen.

([10]) In verband met „rectificeren" wil het CBP duidelijk stellen dat het niet gemachtigd zal zijn om de gegevens van het PNR-bestand waartoe het van de lucthvaartmaatschappijen toegang krijgt, te wijzigen. In plaats daarvan zal een apart bestand met een link naar het PNR-bestand worden gecreëerd om erop te wijzen dat de gegevens onjuist werden geacht en de gecorrigeerde versie ervan te geven. In voorkomend geval zal het CBP het tweede bestand van de passagier voorzien van het commentaar dat bepaalde gegevens in de PNR (misschien) niet correct zijn.

40. Verzoeken om rectificatie van PNR-gegevens in de databank van het CBP en klachten van individuen over de behandeling van hun PNR-gegevens door het CBP kunnen hetzij direct, hetzij via de relevante gegevensbeschermingsautoriteit (voorzover deze daartoe door de betrokkene specifiek is gemachtigd) worden ingediend bij de Assistant Commissioner, Office of Field Operations, US Bureau of Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, DC 20229.

41. Indien een klacht niet door het CBP kan worden afgehandeld, mag deze schriftelijk worden gericht aan de Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, die de zaak zal onderzoeken en het geschil zal trachten te beslechten ([11]).

42. Voorts zal het Privacy Office van het DHS klachten die door gegevensbeschermingsautoriteiten in de lidstaten van de Europese Unie namens een EU-ingezetene naar hem worden doorverwezen, snel in behandeling nemen, voorzover die ingezetene de gegevensbeschermingsautoriteit heeft gemachtigd om namens hem of haar op te treden en van oordeel is dat zijn of haar klacht over de bescherming van PNR-gegevens niet op bevredigende wijze door het CBP (zie de punten 37 tot en met 41 van deze verbintenissen) of door het Privacy Office van het DHS is afgehandeld. Het Privacy Office zal zijn conclusies rapporteren en de gegevensbeschermingsautoriteit(en) over de eventueel te nemen maatregelen adviseren. De Chief Privacy Officer van het DHS zal in haar rapport aan het Congres informatie verstrekken over het aantal, de inhoud en de afhandeling van klachten over de behandeling van persoonlijke gegevens, zoals PNR ([12]).

Nalevingskwesties

43. Het CBP zal, samen met het DHS, eenmaal per jaar of vaker, als de partijen dat overeenkomen, samen met de Europese Commissie, bijgestaan door vertegenwoordigers van Europese rechtshandhavingsinstanties en/of autoriteiten van de lidstaten van de Europese Unie ([13]), deelnemen aan een gemeenschappelijke evaluatie van de uitvoering van deze verbintenissen met als doel een wederzijdse bijdrage te leveren tot de efficiënte werking van de in deze verbintenissen beschreven procedures.

44. Het CBP zal verordeningen, richtsnoeren of andere beleidsdocumenten opstellen waarin de hierbij aangegane verplichtingen worden opgenomen om de naleving van deze verbintenissen door CBP-functionarissen, -werknemers en -contractanten te waarborgen. Zoals reeds vermeld, kan niet naleving van de hierin vervatte beleidsmaatregelen van het CBP door zijn functionarissen, werknemers en contractanten in strenge tuchtmaatregelen en eventueel strafrechtelijke sancties resulteren.

Wederkerigheid

45. Indien in de Europese Unie een identificatiesysteem voor vliegtuigpassagiers wordt ingevoerd, waarbij alle luchtvaartmaatschappijen worden verplicht de autoriteiten toegang te verlenen tot PNR-gegevens voor personen van wie de reis ook een vlucht naar of vanuit de Europese Unie omvat, zal het CBP, strikt op basis van wederkerigheid, de in de Verenigde Staten gevestigde luchtvaartmaatschappijen tot samenwerking aanmoedigen.

Herziening en beëindiging van de verbintenissen

46. Deze verbintenissen gelden voor een periode van drie jaar en zes maanden (3,5 jaar), gerekend vanaf de datum waarop tussen de Verenigde Staten en de Europese Gemeenschap een overeenkomst in werking treedt waarbij de verwerking van PNR gegevens door luchtvaartmaatschappijen met het oog op de doorgifte ervan naar het CBP overeenkomstig de desbetreffende richtlijn wordt toegestaan. Nadat deze verbintenissen twee jaar en zes maanden (2,5 jaar) zijn toegepast, zal het CBP, samen met het DHS, besprekingen gaan voeren met de Commissie om de verbintenissen en alle ter ondersteuning ervan genomen maatregelen onder wederzijds aanvaardbare voorwaarden uit te breiden. Indien geen wederzijds aanvaardbare regeling kan worden getroffen vóór de datum waarop deze verbintenissen verlopen, zullen de verbintenissen vervallen.

([11]) De Chief Privacy Officer van het DHS is onafhankelijk van alle directoraten binnen het Department of Homeland Security. Zij is wettelijk verplicht erop toe te zien dat persoonlijke informatie wordt gebruikt overeenkomstig de relevante wetgeving (zie voetnoot 12). De besluiten van de Chief Privacy Officer zijn bindend voor het Department en kunnen om politieke redenen niet teniet worden gedaan.

([12]) Overeenkomstig sectie 222 van de Homeland Security Act van 2002 (Public Law 107-296 van 25 november 2002) dient de Privacy Officer van het DHS een „privacy-effectbeoordeling" te maken van alle regelgevingsvoorstellen van het Department inzake „de privacy van persoonlijke informatie, met inbegrip van het type verzamelde persoonlijke informatie en het aantal betrokken personen" en het Congres jaarlijks verslag uit te brengen over de „activiteiten van het Department op het gebied van privacy". Sectie 222, lid 5, van bovengenoemde wet bepaalt ook uitdrukkelijk dat de Privacy Officer van het DHS aan het Congres verslag moet uitbrengen over alle „klachten in verband met schendingen van de privacy".

([13]) De samenstelling van de teams aan beide zijden zal van tevoren aan elkaar worden meegedeeld; aan de teams kan worden deelgenomen door relevante autoriteiten die werkzaam zijn op het gebied van privacy/gegevensbescherming, douanecontrole en andere vormen van wetshandhaving, beveiliging van de grenzen en/of de luchtvaart. De deelnemende autoriteiten zal worden verzocht het nodige veiligheidsonderzoek te verrichten en de vertrouwelijkheid van de besprekingen en van de documenten waar ze eventueel toegang toe krijgen, te respecteren. De vertrouwelijkheid belet echter geen van beide partijen om bij hun respectieve bevoegde autoriteiten, waaronder het VS-Congres en het Europees Parlement, naar behoren over de resultaten van de gemeenschappelijke evaluatie te rapporteren. De deelnemende autoriteiten mogen echter in geen geval persoonsgegevens van een betrokkene, niet-publieke informatie uit documenten waartoe zij toegang krijgen, en operationele of interne informatie die zij tijdens de gezamenlijke evaluatie verkrijgen, openbaar maken. Beide partijen zullen in onderling overleg bepalen hoe de gemeenschappelijke evaluatie precies moet worden gerealiseerd.

Geen nieuw particulier recht of precedent

47. Deze verbintenissen leiden niet tot het ontstaan of de overdracht van rechten of voordelen ten gunste van privaat- of publiekrechtelijke personen.

48. De bepalingen van deze verbintenissen zullen geen precedent vormen voor toekomstige besprekingen met de Europese Commissie, de Europese Unie, een aanverwante entiteit of een derde land over de doorgifte van gegevens in enigerlei vorm.

11 mei 2004.

AANHANGSEL A

PNR-gegevenselementen die het CBP van luchtvaartmaatschappijen verlangt

1. PNR-bestandslocatiecode
2. Boekingsdatum
3. Geplande reisdatum (-data)
4. Naam
5. Andere namen in het PNR
6. Adres
7. Alle informatie over de betalingswijzen
8. Factuuradres
9. Telefoonnummers van contactpersonen
10. Volledige reisroute voor dit specifieke PNR
11. Informatie over passagiers die vaak reizen (alleen afgelegde afstand in mijlen en adres(sen))
12. Reisbureau
13. Reisagent
14. Code uitwisseling PNR-informatie
15. Reisstatus passagier
16. Opgesplitste/opgedeelde PNR-informatie
17. E-mailadres
18. Informatie uit het reisbiljetveld
19. Algemene opmerkingen
20 Biljetnummer
21. Zitplaatsnummer
22. Uitgiftedatum reisbiljet
23. „No-show"-antecedenten
24. Bagagebiljetnummers
25. „Go-show"-informatie
26. OSI-informatie (andere informatie over serviceverlening)
27. SSI/SSR-informatie (informatie over bijzondere serviceverlening en de daarbij gestelde eisen)
28. Informatiebron(nen)
29. Alle vroegere wijzigingen van het PNR
30. Aantal reizigers in het PNR
31. Informatie over de zitplaats
32. Enkele-reisbiljetten
33. Alle verzamelde APIS-informatie (Advanced Passenger Information System)
34. ATFQ-velden (Automatic Ticketing Fare Quote: automatische prijsnotering reisbiljet)