

NL

NL

NL



EUROPESE COMMISSIE

Brussel, 21.9.2010
COM(2010) 492 definitief

MEDEDELING VAN DE COMMISSIE

over de algemene aanpak van de doorgifte van passagiersgegevens (Passenger Name Record - PNR) aan derde landen

MEDEDELING VAN DE COMMISSIE

over de algemene aanpak van de doorgifte van passagiersgegevens (Passenger Name Record - PNR) aan derde landen

1. INLEIDING

De terroristische aanslagen in de Verenigde Staten in 2001, in Madrid in 2004 en in Londen in 2005 hebben geleid tot een nieuwe benadering van het binnenlandse veiligheidsbeleid. Recente gebeurtenissen zoals de vrijdelde aanslagen op een vliegtuig op kerstdag 2009 en op Times Square, New York in 2010 wijzen erop dat de terroristische dreiging nog steeds actueel is. Tegelijkertijd neemt de georganiseerde criminaliteit, met name op het gebied van drugs en mensenhandel, steeds toe¹.

Als een reactie op deze voortdurende dreigingen hebben de EU en andere derde landen nieuwe maatregelen genomen, onder meer het verzamelen en uitwisselen van persoonsgegevens. Een overzicht van deze maatregelen heeft de Commissie gegeven in haar Overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht². Het gebruik van passagiersgegevens (PNR-gegevens) voor rechtshandavingsdoeleinden is een van die maatregelen.

Op 16 januari 2003 heeft de Commissie een mededeling gericht aan de Raad en het Europees Parlement over de "doorgifte van passagiersgegevens (PNR-gegevens): een allesomvattende EU-aanpak"³, die beoogde de bouwstenen aan te reiken voor een algemene EU-aanpak op het gebied van PNR-gegevens. In de mededeling werd opgeroepen tot het tot stand brengen van een wettelijk solide kader voor de doorgifte van PNR-gegevens aan het Amerikaanse ministerie van Binnenlandse Veiligheid en tot de vaststelling van een intern beleid op PNR-gebied. Tevens werd opgeroepen tot de ontwikkeling van het "push"-systeem voor de doorgifte van gegevens door de luchtvaartmaatschappijen⁴ en tot een internationaal initiatief voor de doorgifte van PNR-gegevens in het kader van de Internationale Organisatie voor de Burgerluchtvaart (ICAO).

De conclusies van die mededeling zijn voor een groot deel reeds ten uitvoer gelegd; voor andere is de uitvoering nog aan de gang. Meer bepaald heeft de EU met het Amerikaanse ministerie van Binnenlandse Veiligheid een overeenkomst ondertekend betreffende de doorgifte van PNR-gegevens met het oog op de bestrijding van terrorisme en zware grensoverschrijdende criminaliteit, die voorziet in de doorgifte van PNR-gegevens maar tevens de bescherming van persoonsgegevens waarborgt⁵. Daarnaast heeft de Commissie een voorstel aangenomen voor een kaderbesluit over het gebruik van PNR-gegevens voor rechtshandavingsdoeleinden⁶. De Commissie onderzoekt momenteel aan de hand van een effectbeoordeling of het mogelijk is dit voorstel te vervangen door een voorstel voor een richtlijn over het gebruik van PNR-gegevens voor rechtshandavingsdoeleinden. De meeste luchtvaartmaatschappijen hebben het push-systeem voor de doorgifte van gegevens op

¹ Eurostat 36/2009.

² COM(2010) 385.

³ COM(2003) 826.

⁴ Dit houdt in dat de luchtvaartmaatschappij de gegevens aan het derde land doorgeeft, eerder dan een derde land toegang te verlenen tot haar databases.

⁵ PB L 204 van 4.8.2007, blz. 16.

⁶ COM(2007) 654.

adequate wijze ingevoerd, en de ICAO heeft een reeks richtsnoeren uitgewerkt voor de doorgifte van PNR-gegevens.

Naast de overeenkomst met de VS heeft de EU soortgelijke overeenkomsten ondertekend met Canada⁷ en Australië⁸. Nieuw-Zeeland, Zuid-Korea en Japan maken eveneens gebruik van PNR-gegevens maar hebben tot op heden geen overeenkomsten gesloten met de EU. Binnen de EU beschikt het Verenigd Koninkrijk reeds over een PNR-systeem, terwijl andere lidstaten wetgeving op dit gebied hebben aangenomen of tests verrichten met het gebruik van PNR-gegevens.

Deze ontwikkelingen wijzen erop dat het gebruik van PNR-gegevens toeneemt en steeds meer wordt beschouwd als een regulier en noodzakelijk aspect van de rechtshandhaving. Het gebruik van PNR-gegevens impliceert evenwel de verwerking van persoonsgegevens, wat belangrijke vragen oproept in verband met de fundamentele rechten op bescherming van het privéleven en van persoonsgegevens.

De EU staat dan ook voor nieuwe uitdagingen met betrekking tot de internationale doorgifte van PNR-gegevens. Het aantal landen in de wereld die PNR-systemen ontwikkelen, zal in de komende jaren waarschijnlijk nog toenemen. Voorts heeft de EU, door haar ervaring met de gezamenlijke evaluaties van de overeenkomsten met de VS en Canada, een goed inzicht gekregen in de structuur en waarde van PNR-systemen.

De Commissie acht het dan ook noodzakelijk haar algemene aanpak van de doorgifte van PNR-gegevens aan derde landen opnieuw te bekijken. De herziening van haar aanpak moet zorgen voor stevige garanties inzake gegevensbescherming en tot de onverkorte eerbiediging van de grondrechten, en moet stroken met de beleidsontwikkelingsbeginselen die zijn geformuleerd in het overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht⁹. De visie op algemene PNR-vraagstukken van de belangrijkste stakeholders zoals de lidstaten, het Europees Parlement, de Europese Toezichthouder voor gegevensbescherming en de Groep gegevensbescherming artikel 29, zijn bijzonder belangrijk voor de ontwikkeling van de herziene aanpak op het gebied van PNR.

Deze mededeling heeft als belangrijkste doelstelling, voor het eerst een reeks algemene criteria vast te stellen die kunnen dienen als basis voor toekomstige onderhandelingen over PNR-overeenkomsten met derde landen. Dit zal het voor de EU gemakkelijker maken om op de actuele trends in te spelen en tegelijk aan derde landen, aan lidstaten en aan burgers duidelijk maken hoe de Europese Commissie haar externe PNR-beleid vorm wil geven. In aanbevelingen van de Commissie voor onderhandelingen over PNR-overeenkomsten met derde landen moeten in de toekomst minimaal de in deze mededeling vastgelegde algemene criteria in acht worden genomen, waaraan in elke aanbeveling extra criteria kunnen worden toegevoegd.

2. INTERNATIONALE TRENDS OP PNR-GEBIED

2.1. PNR-gegevens en het gebruik ervan

PNR-gegevens zijn niet-geverifieerde informatie die door passagiers is verstrekt en door de luchtvaartmaatschappijen is verzameld met het oog op boekingen en ten behoeve van de incheckprocedure. Het is een weergave van de reisbehoeften van elke passagier zoals die in de boekings- en vertrekcontrolesystemen van de luchtvaartmaatschappijen zijn opgeslagen. De

⁷ PB L 91 van 29.3.2006, blz. 53, PB L 91 van 29.3.2006, blz. 49, en PB L 82 van 21.3.2006, blz. 15.

⁸ PB L 213 van 8.8.2008, blz. 49.

⁹ COM(2010) 385.

PNR-gegevens omvatten verschillende soorten informatie, bijvoorbeeld reisdata en -traject, ticketinformatie, contactgegevens zoals adres en telefoonnummers, reisagent, betalingsinformatie, stoelnummer en bagage-informatie.

De PNR-gegevens zijn niet hetzelfde als de vooraf te verstrekken passagiersgegevens (Advance Passenger Information - API). API-gegevens zijn de biografische informatie die van het machineleesbare gedeelte van een paspoort kan worden afgelezen en omvatten de naam, woonplaats, geboorteplaats en nationaliteit van een persoon. Krachtens de API-richtlijn¹⁰ worden de API-gegevens alleen met het oog op betere grenscontroles en de bestrijding van illegale immigratie aan de grenscontrole instanties doorgegeven bij vluchten die het grondgebied van de EU binnenkomen. Hoewel het gebruik ervan voor andere rechtshandavingsdoeleinden door de richtlijn wordt toegestaan, wordt dit eerder geacht de uitzondering dan de regel te zijn. De gegevens worden door de lidstaten gedurende 24 uur bewaard.

API-gegevens worden hoofdzakelijk gebruikt voor identiteitscontroles als onderdeel van grenscontroles en grensbeheer, maar in bepaalde gevallen worden de gegevens door rechtshandavingsinstanties ook gebruikt om verdachten en gezochte personen te identificeren. API-gegevens worden dus in de eerste plaats gebruikt als een instrument voor identiteitsbeheer. Het gebruik van die gegevens wordt in toenemende mate een overal ter wereld gangbare praktijk. Meer dan 30 landen gebruiken ze systematisch, en in 40 andere is men bezig met het opzetten van API-systemen.

Naast het doorgeven van API-gegevens verlangen sommige landen van de luchtvaartmaatschappijen dat zij hen PNR-gegevens verstrekken. Die gegevens worden vervolgens gebruikt voor de bestrijding van terrorisme en zware criminaliteit, zoals mensenhandel en drugsmokkel. PNR-gegevens worden overal ter wereld al bijna 60 jaar gebruikt, in hoofdzaak door douane instanties maar ook door rechtshandavingsinstanties. Tot kort geleden was het technisch echter niet mogelijk die gegevens elektronisch en vooraf in te zien, zodat het gebruik ervan beperkt bleef tot manuele verwerking voor niet meer dan enkele vluchten. De technologische vooruitgang maakt het thans mogelijk de gegevens vooraf elektronisch door te geven.

Het gebruik dat van PNR-gegevens enerzijds en API-gegevens anderzijds wordt gemaakt, is zeer verschillend, in hoofdzaak omdat ze heel verschillende soorten gegevens omvatten. PNR-gegevens worden vooral gebruikt als een opsporingsinstrument in strafzaken, en niet als een middel voor identiteitscontrole. Het gaat voornamelijk om de volgende vormen van gebruik: (i) risicobeoordeling van passagiers en identificatie van "onbekende" personen, d.w.z. personen die mogelijk de belangstelling van de rechtshandavingsinstanties kunnen wekken en die tot dusver niet verdacht waren, (ii) ze zijn vroeger beschikbaar dan API-gegevens en geven de rechtshandavingsinstanties een voordeel doordat die meer tijd hebben voor verwerking, analyse en follow-upactie, (iii) uitzoeken aan welke personen bepaalde adressen, kredietkaarten e.d. die met strafbare feiten verbonden zijn toebehoren, en (iv) vergelijken van de PNR-gegevens met andere PNR-gegevens ter identificatie van de compagnons van verdachten, bijvoorbeeld door na te gaan wie samen reist.

PNR-gegevens zijn uniek door hun aard en hun gebruik. Dat gebruik kan verschillende vormen aannemen:

¹⁰ Richtlijn 2004/82/EG van 29 augustus 2004 betreffende de verplichting voor vervoerders om passagiersgegevens door te geven.

re-actief (historische gegevens): gebruik bij onderzoeken, strafvervolgning, ontrafelen van netwerken nadat een misdrijf is gepleegd. Om rechtshandavingsinstanties de mogelijkheid te bieden ver genoeg terug te gaan in de tijd, is het in dergelijke gevallen nodig dat de rechtshandavingsinstanties de gegevens gedurende een passende termijn kunnen bewaren;

real-time (actuele gegevens): gebruik om een misdrijf te voorkomen of om personen na te trekken of te arresteren voordat een misdrijf is gepleegd dan wel omdat een misdrijf is of wordt gepleegd. In dergelijke gevallen zijn de PNR-gegevens noodzakelijk om ze te toetsen aan vooraf bepaalde, uit feiten afgeleide risico-indicatoren teneinde de voorheen "onbekende" verdachten te kunnen identificeren en om ze te vergelijken met diverse databases van gezochte personen en voorwerpen;

pro-actief (patronen): gebruik voor trendanalyse en het onderkennen van uit feiten afgeleide reis- en algemene gedragspatronen, die kunnen dienen voor real-time gebruik. Om reis- en gedragspatronen vast te stellen moeten trendanalisten gerechtigd zijn de gegevens gedurende een voldoende lange periode te gebruiken. Een passende termijn voor de bewaring van de gegevens door rechtshandavingsinstanties is in dergelijke gevallen noodzakelijk.

2.2. Actuele trends

Sommige derde landen, zoals de Verenigde Staten, Canada, Australië, Nieuw-Zeeland en Zuid-Korea, gebruiken thans reeds PNR-gegevens voor rechtshandavingsdoeleinden. Andere derde landen hebben wetgeving op dit gebied aangenomen en/of testen momenteel het gebruik van PNR-gegevens, met name Japan, Saudi-Arabië, Zuid-Afrika en Singapore. Verscheidene andere derde landen overwegen op dit ogenblik het gebruik van PNR-gegevens maar hebben nog geen wetgeving ter zake aangenomen. Binnen de EU beschikt het Verenigd Koninkrijk reeds over een PNR-systeem. Frankrijk, Denemarken, België, Zweden en Nederland hebben wetgeving op dit gebied aangenomen en/of testen momenteel het gebruik van PNR-gegevens. Verscheidene andere lidstaten overwegen het opzetten van een PNR-systeem.

De Europese Commissie is zich terdege bewust van de noodzaak van PNR-gegevens voor de voorkoming en bestrijding van terrorisme en zware criminaliteit en heeft, aansluitend bij haar mededeling van 2003, een voorstel voor een kaderbesluit over het gebruik van PNR-gegevens voor rechtshandavingsdoeleinden ingediend. Nu het Verdrag van Lissabon in werking is getreden, overweegt de Commissie dit voorstel te vervangen door een voorstel voor een richtlijn over het gebruik van PNR-gegevens voor rechtshandavingsdoeleinden. Het voorstel zal ertoe strekken luchtvaartmaatschappijen te verplichten PNR-gegevens door te geven aan de lidstaten voor gebruik bij de bestrijding van terrorisme en zware criminaliteit.

Op internationaal niveau wordt steeds meer algemeen aangenomen dat PNR-gegevens een onmisbaar instrument zijn in de strijd tegen terrorisme en zware criminaliteit. Deze trend is de resultante van drie parameters. Ten eerste vormen terrorisme en zware criminaliteit een ernstige bedreiging voor de maatschappij en moeten er maatregelen worden genomen om dit aan te pakken. De toegang tot en analyse van PNR-gegevens is een van de maatregelen die noodzakelijk worden geacht uit een oogpunt van rechtshandhaving. Ten tweede hebben recente technologische ontwikkelingen die toegang en analyse mogelijk gemaakt, wat enkele jaren geleden nog ondenkbaar was. De diverse technologische ontwikkelingen van de laatste jaren worden ook door misdadigers op grote schaal gebruikt bij de planning, voorbereiding en uitvoering van hun misdaden. En ten slotte zorgt – tegen de achtergrond van een steeds toenemend internationaal reisverkeer en een steeds stijgend aantal reizigers – de elektronische verwerking van gegevens vóór de aankomst van de passagiers ervoor dat veiligheids- en grenscontroles veel soepeler en sneller verlopen, omdat het proces van risicoanalyse reeds vooraf heeft plaatsgevonden. Zo kunnen de rechtshandavingsinstanties hun aandacht

exclusief richten op passagiers van wie zij om gegronde redenen aannemen dat ze mogelijk een echt veiligheidsrisico vormen, eerder dan inschattingen te maken op basis van intuïtie, vaste stereotypen of profielen.

2.3. Effecten van de actuele trends voor de Europese Unie

De EU-wetgeving inzake gegevensbescherming staat niet toe dat luchtvaartmaatschappijen die vanuit de EU vliegen de PNR-gegevens van hun passagiers doorgeven aan derde landen waar het niveau van bescherming van persoonsgegevens ontoereikend is, zonder dat passende waarborgen worden gegeven. Toen de Verenigde Staten, Canada en Australië de luchtvaartmaatschappijen vroegen PNR-gegevens door te geven bij vluchten naar hun landen, kwamen de luchtvaartmaatschappijen bijgevolg in een zeer lastig parket. Daarom is de EU onderhandelingen aangegaan en heeft zij uiteindelijk afzonderlijke internationale overeenkomsten gesloten met elk van deze drie landen¹¹, waardoor de doorgifte van PNR-gegevens buiten de EU aan rechtshandavingsinstanties van de genoemde drie landen mogelijk werd gemaakt. Dit gebeurde om de luchtvaartmaatschappijen uit de nood te helpen, om de passagiers een passend niveau van gegevensbescherming te waarborgen en als erkenning van de noodzaak en het belang van het gebruik van PNR-gegevens bij de bestrijding van terrorisme en zware criminaliteit.

Aangezien steeds meer landen PNR-systemen invoeren, zal dit probleem zich naar verwachting blijven voordoen. Als de Commissie besluit werk te maken van een voorstel voor een EU-richtlijn inzake PNR-gegevens, zou de frequentie van dergelijke verzoeken nog kunnen toenemen, wanneer derde landen van de EU wederkerigheid verlangen.

Tot dusver werden internationale overeenkomsten met derde landen op PNR-gebied "vraaggestuurd" gesloten en geval per geval bekeken. Ofschoon alle overeenkomsten dezelfde problemen behandelen en dezelfde punten regelen, zijn de bepalingen ervan niet identiek. Dit heeft ertoe geleid dat de regels voor luchtvaartmaatschappijen en inzake gegevensbescherming soms uiteenlopen. Aangezien de "vraag" in de nabije toekomst waarschijnlijk nog zal toenemen, zou de EU er goed aan doen een strategie te ontwikkelen om deze vraag op een meer gestructureerde wijze tegemoet te treden, met geringere verschillen tussen de diverse overeenkomsten tot gevolg.

3. EEN HERZIENE ALGEMENE EU-AANPAK OP PNR-GEBIED

3.1. Motivering voor een herziene algemene aanpak op PNR-gebied

De conclusies van de mededeling van 2003 worden thans volop uitgevoerd. Nu de EU geconfronteerd wordt met nieuwe trends en uitdagingen, is het belangrijk dat zij daarmee rekening houdt door haar algemene aanpak met betrekking tot de doorgifte van PNR-gegevens aan derde landen verder te ontwikkelen, en wel om de volgende redenen:

Bestrijding van terrorisme en zware grensoverschrijdende criminaliteit: de EU is het zichzelf en derde landen verplicht met hen samen te werken bij de bestrijding van deze dreigingen. Eén manier van samenwerken is het uitwisselen van gegevens met derde landen. PNR-gegevens ter beschikking stellen voor rechtshandavingsdoeleinden is een noodzakelijk

¹¹ PNR-overeenkomst EG-VS 2004 (PB L 183 van 20.5.2004, blz. 84) en Beschikking van de Commissie van 14 mei 2004 (PB L 235 van 6.7.2004, blz. 11); PNR-overeenkomst EU-VS 2006 (PB L 298 van 27.10.2006, blz. 29) en begeleidende brieven (PB C 259 van 27.10.2006, blz. 1), PNR-overeenkomst EU-VS 2007 (PB L 204 van 4.8.2007, blz. 18), PNR-overeenkomst EU-Canada (PB L 82 van 21.3.2006, blz. 15 en PB L 91 van 29.3.2006, blz. 49) en PNR-overeenkomst EU-Australië (PB L 213 van 8.8.2008, blz. 47).

hulpmiddel voor de bestrijding van terrorisme en zware grensoverschrijdende criminaliteit. Zowel in de strategie voor de externe dimensie van justitie en binnenlandse zaken¹² als in de terrorismebestrijdingsstrategie van de EU¹³ en het programma van Stockholm¹⁴ wordt melding gemaakt van de noodzaak van nauwe samenwerking met derde landen.

Bescherming van persoonsgegevens en de persoonlijke levenssfeer: de EU heeft zich verbonden tot een effectief, hoog niveau van bescherming van persoonsgegevens, en onder meer te verzekeren dat elke doorgifte van PNR-gegevens aan derde landen veilig en in overeenstemming met de bestaande wettelijke voorschriften van de EU verloopt en dat passagiers hun rechten met betrekking tot de verwerking van hun gegevens kunnen afdwingen.

Behoeft e aan rechtszekerheid en aan eenvormige verplichtingen voor de luchtvaartmaatschappijen: het is belangrijk dat de EU een samenhangend rechtskader biedt voor het doorgeven van PNR-gegevens door luchtvaartmaatschappijen aan derde landen. Dit is noodzakelijk om te voorkomen dat de luchtvaartmaatschappijen sancties oplopen alsook om de voorwaarden en procedures voor het doorgeven van gegevens wereldwijd zo eenvormig en geharmoniseerd mogelijk te maken, zodat de kosten voor de ondernemingen dalen en er in de sector gelijke mededingingsvoorwaarden gelden.

Vaststelling van algemene voorwaarden met het oog op de samenhang en de verdere ontwikkeling van een internationale aanpak: de PNR-overeenkomsten die de EU met derde landen heeft ondertekend, hebben een vergelijkbaar oogmerk maar de inhoud ervan verschilt wat betreft de praktische regeling van de doorgiften en de aard van de verplichtingen van het derde land. Dat verschil in verplichtingen is tot op zekere hoogte aanvaardbaar gezien de verschillende vereisten en de verschillende rechtsorde in elk van de betrokken landen, maar ze zouden steeds aan bepaalde algemene criteria moeten voldoen (zie de punten 3.2 en 3.3). Met het oog op een zo eenvormig mogelijke behandeling van de passagiers en het beperken van de kosten voor de ondernemingen is het van belang dat de inhoud van en de normen in toekomstige overeenkomsten zo gelijk mogelijk zijn. Dat zou dan de basis kunnen vormen voor een volgende stap, die zou kunnen bestaan in een meer geharmoniseerde multilaterale aanpak van de uitwisseling van PNR-gegevens.

Bijdragen tot een groter gemak voor de reizigers: om de veiligheidsdreigingen die in onze samenlevingen aanwezig zijn aan te pakken, worden de passagiers bij het overschrijden van grenzen steeds grondiger en langduriger gecontroleerd. Samen met de voortdurende toename van het internationale reisverkeer leidt dit tot het ontstaan van langere wachttijden aan de grenzen. De voorafgaande elektronische doorgifte van PNR-gegevens, vóór de eigenlijke grensoverschrijding, maakt het mogelijk de passagierscontroles vooraf te verrichten, zodat de grensovergang sneller en met minder hinder kan verlopen, terwijl de rechtshandavingsinstanties zich uitsluitend hoeven te concentreren op de personen die als belangwekkend zijn geïdentificeerd.

3.2. Algemene overwegingen

De herziene algemene aanpak op PNR-gebied moet de basis worden op grond waarvan de EU beslist hoe in de toekomst het best kan worden omgegaan met verzoeken van derde landen om doorgifte van PNR-gegevens. Naast de beginselen inzake beleidsontwikkeling die in het overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht zijn beschreven, zijn daarbij de volgende specifieke overwegingen van belang:

¹² COM(2005) 491.

¹³ Raadsdocument 14469/4/05 van 30.11.2005.

¹⁴ Raadsdocument 17024/09 van 2.12.2009.

Gedeelde veiligheidsbelangen: terrorisme en zware criminaliteit zijn internationaal van aard. Sommige landen in de wereld staan meer dan andere bloot aan de toenemende dreiging van terrorisme en zware criminaliteit. De EU is vastbesloten met hen samen te werken en hen bij te staan bij het bestrijden van deze veiligheidsdreigingen.

Bescherming van persoonsgegevens: aangezien de doorgifte, het gebruik en de verwerking van PNR-gegevens het grondrecht van individuen op bescherming van hun persoonsgegevens raakt, is het van cruciaal belang dat de EU uitsluitend medewerking verleent aan derde landen die voor de uit de EU afkomstige PNR-gegevens een passend beschermingsniveau kunnen waarborgen.

Externe betrekkingen: ook de aard van de betrekkingen die de EU in het algemeen met het derde land onderhoudt, speelt een rol. Het functioneren van en de samenwerking met politie en rechterlijke instanties, alsook de inachtneming van de beginselen van de rechtsstaat en van de grondrechten zijn daarbij belangrijke criteria.

3.3. Normen, inhoud en criteria

In het kader van de algemene PNR-aanpak dient te worden bepaald aan welke algemene normen internationale overeenkomsten tussen de EU en derde landen moeten voldoen met het oog op een zo groot mogelijke samenhang in de door die landen te verstrekken garanties inzake gegevensbescherming en in de praktische regeling van de doorgifte van de gegevens door de luchtvaartmaatschappijen.

Het is tevens van cruciaal belang dat de EU beschikt over mechanismen om toezicht te houden op de correcte naleving, bijvoorbeeld door een periodieke gezamenlijke evaluatie van de uitvoering van de overeenkomsten en effectieve systemen voor het beslechten van geschillen.

3.3.1. Bescherming van persoonsgegevens

Het verzamelen en doorgeven van PNR-gegevens aan derde landen betreft een zeer groot aantal personen en hun persoonsgegevens. Er moet derhalve bijzonder veel aandacht worden besteed aan de effectieve bescherming van persoonsgegevens.

In Europa zijn de fundamentele rechten op eerbiediging van het privéleven en op bescherming van persoonsgegevens neergelegd in artikel 8 van het Europees mensenrechtenverdrag (EVRM) en in de artikelen 7 en 8 van het Handvest van de grondrechten van de EU¹⁵. Deze grondrechten gelden voor elke persoon ongeacht nationaliteit of verblijfplaats. Bijkomende normen inzake gegevensbescherming zijn vastgelegd in Verdrag nr. 108 van de Raad van Europa van 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens en het daarbij behorende aanvullende protocol nr. 181 uit 2001.

Beperkingen op de uitoefening van de in het Handvest erkende rechten en vrijheden moeten bij wet worden gesteld en de wezenlijke inhoud van deze rechten en vrijheden eerbiedigen.

¹⁵ Op te merken valt dat soortgelijke beginselen inzake gegevensbescherming zijn neergelegd in internationale instrumenten betreffende de bescherming van het privéleven en persoonsgegevens, bijvoorbeeld: artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten van 16 december 1966, de UN Guidelines for the Regulation of Computerized Personal Data Files (Resolutie 45/95 van de Algemene Vergadering van de VN van 14 december 1990), de aanbeveling van de OESO-Raad voor richtsnoeren voor de bescherming van de persoonlijke levenssfeer en van grensoverschrijdend verkeer van persoonsgegevens en het Verdrag van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108), alsmede het daarbij behorende Aanvullend Protocol (ETS nr. 181), die ook zijn opgesteld voor ondertekening door niet-Europese staten.

Met inachtneming van het evenredigheidsbeginsel kunnen alleen beperkingen worden gesteld, indien zij noodzakelijk zijn en aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen beantwoorden.

Aangezien de beschermingsregelingen in derde landen kunnen verschillen van de in de EU geldende gegevensbescherming, is het van belang dat voor elke doorgifte van PNR-gegevens van EU-lidstaten naar derde landen het betrokken derde land op basis van een solide rechtsgrondslag een toereikend niveau van gegevensbescherming waarborgt. Dat toereikende niveau van gegevensbescherming kan ofwel zijn vastgelegd in de wetgeving van het derde land, ofwel worden verschaft in de vorm van in rechte afdwingbare verbintenissen in de internationale overeenkomst met betrekking tot de verwerking van persoonsgegevens.

Of de door een derde land geboden bescherming toereikend is, moet worden beoordeeld met inachtneming van alle omstandigheden die verband houden met de doorgifte van gegevens. In dit verband zal de EU ook nagaan of het derde land de internationale normen in acht neemt, en meer bepaald of het internationale instrumenten inzake gegevensbescherming en grondrechten in het algemeen heeft geratificeerd. Besluiten die de Commissie over dit onderwerp reeds heeft genomen, dienen als leidraad te worden gebruikt om te bepalen wat als toereikend kan worden beschouwd.

De basisbeginselen voor de bescherming van persoonsgegevens die het aanvragende derde land in acht moet nemen, zijn:

- **Beperking van de doeleinden – gebruik van de gegevens:** de omvang van het gebruik dat een derde land van de gegevens wil maken, moet duidelijk en nauwkeurig worden omschreven in de overeenkomst en mag niet ruimer zijn dan wat nodig is voor de te bereiken doeleinden. De ervaring met de bestaande PNR-overeenkomsten leert dat PNR-gegevens uitsluitend horen te worden gebruikt voor rechtshandavings- en beveiligingsdoeleinden in het kader van de bestrijding van terrorisme en zware grensoverschrijdende criminaliteit. Sleutelbegrippen als terrorisme en zware grensoverschrijdende criminaliteit moeten worden gedefinieerd op basis van de definities die in relevante EU-instrumenten zijn opgenomen.
- **Beperking van de doeleinden – soort gegevens:** de uitwisseling van gegevens moet beperkt blijven tot het minimum en moet evenredig zijn. Elke overeenkomst moet uitputtend de categorieën PNR-gegevens vermelden die moeten worden doorgegeven.
- **Bijzondere categorieën persoonsgegevens (gevoelige gegevens):** PNR-gegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt of die de gezondheid of het seksuele leven betreffen, mogen niet worden gebruikt tenzij onder uitzonderlijke omstandigheden, wanneer er een onmiddellijk gevaar is voor het verlies van mensenlevens en mits het derde land passende waarborgen biedt, bijvoorbeeld dat over het gebruik van de betrokken gegevens steeds geval per geval zal worden beslist, na goedkeuring door een hooggeplaatste ambtenaar, en dat het gebruik strikt beperkt blijft tot de doeleinden van de oorspronkelijke doorgifte.
- **Gegevensbeveiliging:** PNR-gegevens moeten tegen misbruik en onrechtmatige toegang worden beschermd met alle geschikte technische hulpmiddelen, beveiligingsprocedures en maatregelen ter voorkoming van risico's voor de veiligheid, vertrouwelijkheid of integriteit van de gegevens.
- **Toezicht en verantwoording:** om te zorgen dat controle wordt uitgeoefend op de overheidsinstanties die PNR-gegevens gebruiken, moet worden voorzien in een systeem van toezicht door een onafhankelijke overheidsinstantie die verantwoordelijk is voor

gegevensbescherming en die over effectieve handhavingsbevoegdheden beschikt. De eerstgenoemde instanties moeten kunnen worden aangesproken op de naleving van de geldende voorschriften inzake de bescherming van persoonsgegevens en moeten bevoegd zijn om kennis te nemen van klachten van individuele personen betreffende de verwerking van persoonsgegevens.

- **Transparantie en kennisgeving:** eenieder moet minstens te horen krijgen waarom zijn persoonsgegevens worden verwerkt, wie die gegevens zal verwerken, volgens welke regels of wettelijke bepalingen, aan welk soort derden de gegevens zullen worden bekendgemaakt en hoe en bij wie hiertegen kan worden opgekomen.
- **Toegang, rectificatie en wissing:** eenieder moet toegang hebben tot zijn PNR-gegevens en het recht hebben die in voorkomend geval te laten corrigeren of wissen.
- **Beroepsmogelijkheid:** eenieder moet, op niet-discriminerende wijze en ongeacht zijn nationaliteit of verblijfplaats, het recht hebben om bij een administratieve of rechterlijke instantie beroep in te stellen wanneer inbreuk is gemaakt op zijn privéleven of de regels inzake gegevensbescherming zijn overtreden. Elke dergelijke inbreuk of overtreding moet worden bestraft met passende en doeltreffende sancties en/of andere maatregelen.
- **Geautomatiseerde individuele besluiten:** besluiten die voor een persoon tot ongunstige maatregelen of effecten leiden, mogen niet uitsluitend gebaseerd zijn op de automatische verwerking van persoonsgegevens, zonder menselijke tussenkomst.
- **Bewaren van gegevens:** de bewaringstermijn voor PNR-gegevens mag niet langer zijn dan noodzakelijk is voor de uitvoering van de beschreven taken. Bij het vaststellen van de bewaringstermijn moet rekening worden gehouden met de verschillende wijzen waarop PNR-gegevens worden gebruikt (zie punt 1.2.1) en met de mogelijkheid om de toegangsrechten in de loop van de bewaringstermijn te beperken, bijvoorbeeld door geleidelijke anonimisering van de gegevens.
- **Beperkingen op verdere doorgifte aan andere overheidsinstanties:** PNR-gegevens mogen uitsluitend worden verstrekt aan andere overheidsinstanties met bevoegdheden op het gebied van de bestrijding van terrorisme en zware grensoverschrijdende criminaliteit die, op grond van een tegenover de ontvangende instantie aangegane verbintenis, dezelfde bescherming bieden als de ontvangende instantie conform de overeenkomst zelf biedt. PNR-gegevens mogen nooit als pakket worden doorgegeven, maar alleen geval per geval.
- **Beperkingen op verdere doorgifte aan derde landen:** het gaat hier in de eerste plaats om beperkingen op het gebruik en de verdere verspreiding om te voorkomen dat de overeenkomst wordt omzeild wanneer PNR-gegevens aan een ander derde land worden doorgegeven. Dergelijke verdere doorgifte moet met passende waarborgen worden omringd. Met name het ontvangende derde land mag deze informatie uitsluitend aan een bevoegde instantie van een ander derde land doorgeven als deze laatste zich ertoe verbindt bij de behandeling van de gegevens hetzelfde beschermingsniveau te waarborgen als in de overeenkomst is voorgeschreven, en de doorgifte strikt beperkt blijft tot de doeleinden van de oorspronkelijke doorgifte van gegevens. PNR-gegevens mogen nooit als pakket worden doorgegeven, maar alleen geval per geval.

3.3.2. *Praktische regeling van de doorgifte*

Met het oog op de rechtszekerheid en een zo gering mogelijk financiële last voor de luchtvaartmaatschappijen is het van belang dat de regels betreffende de wijze waarop de luchtvaartmaatschappijen gegevens doorgeven aan derde landen worden geharmoniseerd. Als de verplichtingen eenvormig zouden zijn, zou dit de financiële last voor de

luchtvaartmaatschappijen sterk verminderen, aangezien zij minder investeringen zouden moeten doen om aan hun verplichtingen te voldoen. Met het oog daarop zou het wenselijk zijn minstens de volgende praktische regelingen betreffende de doorgiften te standaardiseren:

- **De wijze van doorgeven:** om de gegevens in de databases van de luchtvaartmaatschappijen te beschermen en te zorgen dat deze de controle erover behouden, mogen gegevens uitsluitend via een push-systeem worden doorgegeven.
- **De frequentie van de doorgiften:** er moet een redelijke beperking staan op het aantal keren dat het derde land kan verzoeken om doorgifte van de gegevens, waarbij voldoende nut voor de veiligheid moet worden verzoend met zo laag mogelijke kosten voor de luchtvaartmaatschappijen.
- **Geen verplichting voor de luchtvaartmaatschappijen om extra gegevens te verzamelen:** van de luchtvaartmaatschappijen mag niet worden verlangd dat ze meer gegevens verzamelen dan ze reeds doen of dat ze verplicht bepaalde soorten gegevens verzamelen, maar uitsluitend dat ze doorgeven wat ze reeds aan gegevens verzamelen in het kader van hun activiteiten.

3.3.3. Algemene begrippen

- **Geldigheidsduur en herziening:** de overeenkomst over samenwerking met derde landen moet gelden voor een vaste termijn en moet voorzien in de mogelijkheid van opzegging door elk van de partijen. Het moet mogelijk zijn de samenwerkingsregels te herzien indien dat wenselijk wordt geacht.
- **Monitoring:** het is van wezenlijk belang dat de EU beschikt over mechanismen om toe te zien op de correcte naleving, bijvoorbeeld door middel van periodieke gezamenlijke evaluaties van de tenuitvoerlegging van de overeenkomsten in al hun aspecten, waaronder de beperking qua doeleinden, de rechten van passagiers en de verdere doorgifte van PNR-gegevens, en waarbij onder meer een evenredigheidstoetsing van de bewaarde gegevens plaatsvindt op basis van hun waarde voor het bereiken van de doeleinden waarvoor de gegevens zijn doorgegeven. De resultaten van die gezamenlijke evaluaties dienen aan de Raad en het Europees Parlement te worden voorgelegd.
- **Beslechting van geschillen:** er dient te worden voorzien in doeltreffende systemen van geschillenbeslechting met betrekking tot de interpretatie, toepassing en tenuitvoerlegging van de overeenkomsten.
- **Wederkerigheid:** er moet worden gezorgd voor wederkerigheid, met name doordat analytische informatie die uit de PNR-gegevens is afgeleid, door de bevoegde autoriteiten van het ontvangende derde land wordt doorgegeven aan de politieke en justitiële autoriteiten van de lidstaten, alsmede aan Europol en Eurojust.

4. EEN PERSPECTIEF OP LANGERE TERMIJN.

Aangezien wereldwijd meer en meer landen PNR-gegevens gebruiken, hebben de problemen die met dat gebruik gepaard gaan gevolgen voor de hele internationale gemeenschap. De bilaterale aanpak waarvoor de EU indertijd heeft gekozen, was onder de gegeven omstandigheden wellicht de beste keuze en zal dit voor de nabije toekomst waarschijnlijk ook blijven, maar naarmate meer landen PNR-gegevens gaan gebruiken zal daaraan allicht een einde komen. De EU moet dan ook de mogelijkheid onderzoeken om op internationaal niveau normen vast te stellen voor de doorgifte en het gebruik van PNR-gegevens. De richtsnoeren over toegang tot PNR-gegevens die door de ICAO in 2004 zijn ontwikkeld, vormen een solide basis voor de harmonisatie van de praktische regelingen betreffende het doorgeven van PNR-

gegevens. Die richtsnoeren zijn evenwel niet bindend en geven geen afdoende antwoord op vragen in verband met gegevensbescherming. Ze zijn op zichzelf dan ook niet toereikend maar dienen eerder te worden gebruikt als leidraad, met name inzake kwesties die voor de luchtvaartmaatschappijen van belang zijn.

Om die reden moet de EU derhalve overwegen besprekingen te starten met internationale partners die PNR-gegevens gebruiken of de intentie daartoe hebben, ten einde na te gaan of zij voldoende op één lijn zitten om de doorgifte van PNR-gegevens op multilateraal niveau te regelen. Als deze besprekingen goed verlopen, moet de EU formele onderhandelingen aangaan met de belangstellende internationale partners om een multilaterale regeling uit te werken.

5. CONCLUSIE

In deze mededeling werd een overzicht gegeven van de actuele trends in het gebruik van PNR-gegevens in de EU en de wereld. Om in te spelen op deze trends en te reageren op de dreigingen waarmee de EU en de wereld nog steeds geconfronteerd worden, moet de EU, naar het oordeel van de Commissie, haar algemene aanpak op PNR-gebied herzien. Daarbij houdt de Commissie rekening met de visie van de belangrijkste stakeholders op algemene PNR-vraagstukken en met de beginselen op het gebied van beleidsontwikkeling die zijn neergelegd in het overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht.

In deze mededeling worden voor het eerst een aantal algemene ideeën op een rijtje gezet, die voor de EU een richtsnoer zouden moeten vormen bij onderhandelingen met derde landen over PNR-overeenkomsten. Als die beginselen worden nageleefd, zou dit moeten leiden tot een grotere samenhang tussen de verschillende PNR-overeenkomsten en tevens moeten waarborgen dat de grondrechten inzake eerbiediging van het privéleven en bescherming van persoonsgegevens in acht worden genomen. Tegelijk blijft de mededeling voldoende soepel en aanpasbaar aan de specifieke veiligheidsproblemen en de nationale rechtsorde van elk derde land.

Op langere termijn vooruitblikkend op de ontwikkeling van PNR-initiatieven overal in de wereld, komt deze mededeling ten slotte tot de conclusie dat de EU de mogelijkheid moet onderzoeken om op middellange termijn de bilaterale overeenkomsten te vervangen door een multilaterale overeenkomst tussen alle landen die PNR-gegevens gebruiken.