

I

(Resoluties, aanbevelingen en adviezen)

ADVIEZEN

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING

Advies van de Europese Toezichthouder voor gegevensbescherming betreffende het voorstel voor een kaderbesluit van de Raad over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor wetshandavingsdoeleinden

(2008/C 110/01)

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap, en met name op artikel 286,

Gelet op het Handvest van de grondrechten van de Europese Unie, en met name op artikel 8,

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⁾,

Gelet op Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens ⁽²⁾, en met name op artikel 41,

Gezien het verzoek van de Europese Commissie om advies op grond van artikel 28, lid 2, van Verordening (EG) nr. 45/2001 dat op 13 november 2007 is ontvangen;

BRENGT HET VOLGENDE ADVIES UIT:

I. INLEIDING

Raadpleging van de EDPS

1. Het voorstel voor een kaderbesluit van de Raad over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor wetshandavingsdoeleinden (hierna „het voor-

stel”) is door de Commissie op grond van artikel 28, lid 2, van Verordening (EG) nr. 45/2001 voor advies aan de EDPS toegezonden.

2. Het voorstel betreft de verwerking van PNR-gegevens binnen de EU en houdt nauw verband met andere regelingen voor het verzamelen en gebruiken van passagiersgegevens, met name de Overeenkomst tussen de EU en de Verenigde Staten van juli 2007. Deze regelingen zijn van groot belang voor de EDPS, die ook reeds de gelegenheid heeft gehad een aantal eerste opmerkingen te maken over de vragenlijst van de Commissie betreffende het geplande PNR-systeem van de EU, die in december 2006 aan de belanghebbenden is gezonden ⁽³⁾. De EDPS is ermee ingenomen dat hij door de Commissie wordt geraadpleegd. Hij vindt dat dit advies in de preambule van het Raadsbesluit moet worden vermeld.

De context van het voorstel

3. Doel van het voorstel is de harmonisatie van de bepalingen van de lidstaten inzake de verplichtingen van luchtvervoerders die vluchten uitvoeren naar of vanaf het grondgebied van ten minste één lidstaat, om PNR-gegevens door te geven aan de bevoegde autoriteiten met het oog op de voorkoming en bestrijding van terroristische misdrijven en georganiseerde criminaliteit.
4. De Europese Unie heeft met de Verenigde Staten en ook met Canada overeenkomsten gesloten met het oog op de doorgifte van PNR-gegevens voor vergelijkbare doeleinden. Een eerste, in mei 2004 met de Verenigde Staten gesloten,

⁽¹⁾ PB L 281 van 23.11.1995, blz. 31.⁽²⁾ PB L 8 van 12.1.2001, blz. 1.⁽³⁾ Waaronder de lidstaten, de gegevensbeschermingsautoriteiten en luchtvaartmaatschappijen. Deze vragenlijst was opgemaakt met het oog op de opstelling van een effectbeoordeling van het onderhavige voorstel door de Europese Commissie.

overeenkomst is in juli 2007 vervangen door een nieuwe overeenkomst ⁽¹⁾. Een soortgelijke overeenkomst is in juli 2005 met Canada gesloten ⁽²⁾. Voorts gaan weldra onderhandelingen tussen de EU en Australië van start met het oog op een overeenkomst over de uitwisseling van PNR-gegevens; Zuid-Korea verzoekt ook om PNR-gegevens van vluchten naar zijn grondgebied, maar in dit stadium zijn er nog geen plannen voor onderhandelingen op Europees niveau.

5. Binnen de EU vormt het voorstel een aanvulling op Richtlijn 2004/82/EG van de Raad ⁽³⁾ betreffende de verplichting voor vervoerders om passagiersgegevens, bekend als API-gegevens, door te geven met het oog op bestrijding van illegale immigratie en verbetering van de grenscontrole. Deze richtlijn had uiterlijk op 5 september 2006 in het nationale recht van de lidstaten omgezet moeten zijn. Ze wordt evenwel nog niet in alle lidstaten toegepast.

6. In tegenstelling tot de op voorhand af te geven passagiersgegevens (API-gegevens), die moeten helpen bij het identificeren van individuele personen, dragen de in het voorstel vermelde PNR-gegevens bij tot het uitvoeren van risicobeoordelingen van personen, het verkrijgen van inlichtingen en het leggen van verbanden tussen bekende en onbekende personen.

7. Het voorstel bevat de volgende hoofdelementen:

- het voorziet in het beschikbaar stellen door luchtvervoerders van PNR-gegevens aan de bevoegde autoriteiten van de lidstaten met het oog op de voorkoming en bestrijding van terroristische misdrijven en georganiseerde criminaliteit;
- het voorziet in principe in de aanwijzing, in iedere lidstaat, van een passagiersinformatie-eenheid (PIU) die verantwoordelijk is voor het verzamelen van de PNR-gegevens van luchtvervoerders (of door dezen aangewezen intermediairs) en voor het uitvoeren van een risicobeoordeling van de passagiers;
- de dienovereenkomstig beoordeelde informatie zal worden doorgezonden aan de bevoegde autoriteiten in iedere lidstaat. Deze informatie zal per geval en voor het hierboven aangegeven doel worden uitgewisseld met andere lidstaten;
- aan de doorgifte aan landen buiten de Europese Unie zijn bijkomende voorwaarden verbonden;

⁽¹⁾ Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en overdracht van persoonsgegevens van passagiers (PNR-gegevens) door luchtvaartmaatschappijen aan het *Department of Homeland Security* (ministerie van Binnenlandse Veiligheid) van de Verenigde Staten van Amerika (PNR-Overeenkomst van 2007) (PB L 204 van 4.8.2007, blz. 18).

⁽²⁾ Overeenkomst tussen de Europese Gemeenschap en de regering van Canada inzake de verwerking van op voorhand af te geven passagiersgegevens en persoonsgegevens van passagiers (PB L 82 van 21.3.2006, blz. 15).

⁽³⁾ Richtlijn 2004/82/EG van de Raad van 29 april 2004 betreffende de verplichting voor vervoerders om passagiersgegevens door te geven (PB L 261 van 6.8.2004, blz. 24).

— de gegevens worden dertien jaar bewaard, waarvan acht in een slappende databank;

— de verwerking wordt geregeld door het (ontwerp-) kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politieke en justitiële samenwerking in strafzaken (hierna „het kaderbesluit gegevensbescherming”) ⁽⁴⁾;

— een comité met vertegenwoordigers van de lidstaten zal de Commissie bijstaan op het gebied van protocollen en versleuteling, alsook op het gebied van risicobeoordelingscriteria en -praktijken;

— het besluit moet binnen drie jaar na zijn inwerkingtreding worden geëvalueerd.

Invalshoek van het advies

8. Het voorstel waarover de EDPS wordt geraadpleegd, is een verdere stap op weg naar een routinematige verzameling van gegevens van personen die in principe niet van een misdrijf worden verdacht. Zoals hierboven vermeld, speelt deze ontwikkeling zich op internationaal en Europees niveau af.

9. De EDPS neemt er nota van dat ook de Groep van artikel 29 en de Groep politie en justitie een gezamenlijk advies over het voorstel hebben ingediend ⁽⁵⁾. De EDPS steunt dat advies. In het onderhavige advies wordt een aantal aanvullende punten benadrukt en ontwikkeld.

10. Alle relevante aspecten van het voorstel zullen in het advies van de EDPS worden onderzocht, maar de aandacht zal vooral uitgaan naar vier hoofdpunten:

— ten eerste, de rechtmatigheid van de beoogde maatregelen. De vraag naar het doel, de noodzakelijkheid en de evenredigheid van het voorstel zal worden beoordeeld aan de hand van de criteria van artikel 8 van het Handvest van de Grondrechten van de Europese Unie;

— in het advies zal ook worden nagegaan welk recht van toepassing is op de voorgenomen verwerking. Met name het toepassingsgebied van het kaderbesluit gegevensbescherming in verband met de toepassing van de wetgeving inzake gegevensbescherming van de eerste pijler verdient bijzondere aandacht. Het gevolg van de toepasselijke gegevensbeschermingsregeling met betrekking tot de uitoefening van de rechten van de betrokkene zal ook worden bezien;

⁽⁴⁾ De laatste tekst betreffende dit voorstel is in het register van de Raad beschikbaar onder nummer 16397/07.

⁽⁵⁾ Gezamenlijk advies over het door de Commissie op 6 november 2007 ingediende voorstel voor een kaderbesluit van de Raad over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor wetshandhavingsdoeleinden, aangenomen door de Groep van artikel 29 op 5 december 2007 en door de Groep politie en justitie op 18 december 2007, WP 145, WPPJ 01/07.

- vervolgens zal dieper worden ingegaan op de kwaliteit van de ontvangers van gegevens op nationaal niveau. Zo geeft de kwaliteit van de PIU's, de intermediairs en de bevoegde autoriteiten die zijn aangewezen om risicobeoordelingen te verrichten en passagiersgegevens te analyseren, aanleiding tot specifieke bezorgdheid, aangezien het voorstel in dit verband geen precieze gegevens bevat;
- het vierde hoofdpunt betreft de voorwaarden voor doorgifte van gegevens aan derde landen. Het is niet duidelijk welke voorwaarden voor deze doorgifte zullen gelden wanneer er verschillende reeksen regels bestaan: de voorwaarden voor doorgifte van het onderhavige voorstel, samen met die van het kaderbesluit gegevensbescherming, en de bestaande internationale overeenkomsten (met de Verenigde Staten en Canada).

11. In een laatste deel zullen nog andere belangrijke punten aan bod komen, waaronder positieve maatregelen op het gebied van gegevensbescherming, maar ook bijkomende redenen tot bezorgdheid over het voorstel.

II. RECHTMATIGHEID VAN DE VOORGESTELDE MAATREGELEN

12. Om de rechtmatigheid van de voorgestelde maatregelen conform de fundamentele beginselen inzake gegevensbescherming, met name artikel 8 van het Europees Handvest van de Grondrechten en de artikelen 5 tot en met 8 van Verdrag nr. 108 van de Raad van Europa ⁽¹⁾ na te gaan, moet het doel van de beoogde verwerking van persoonsgegevens duidelijk worden vastgesteld, zodat de noodzakelijkheid en de evenredigheid ervan kunnen worden beoordeeld. Er moet worden gegarandeerd dat er geen andere, minder indringende, middelen beschikbaar zijn om het beoogde doel te bereiken.

Bepaling van het doel

13. Uit de formulering van het voorstel en de effectbeoordeling daarvan blijkt dat niet wordt beoogd personen die bekend staan als terrorist of bij de georganiseerde misdaad betrokken crimineel te identificeren door hun namen te vergelijken met de namen die op door de wetshandhavinginstanties beheerde lijsten staan. Het doel is het verzamelen van inlichtingen met betrekking tot terrorisme of georganiseerde criminaliteit, en meer specifiek „het uitvoeren van risicobeoordelingen van personen, het verkrijgen van inlichtingen en het leggen van verbanden tussen bekende en onbekende personen” ⁽²⁾. Het in artikel 3, lid 5, van het voorstel genoemde doel is, in dezelfde lijn en in de eerste plaats, „het identificeren van personen die betrokken zijn of kunnen zijn bij een terroristisch misdrijf of een misdrijf dat verband houdt met georganiseerde criminaliteit en van met deze personen geassocieerde personen”.
14. Dit is de reden die wordt aangehaald om te stellen dat API-gegevens niet volstaan voor het genoemde doel. Zoals reeds is vermeld, kunnen API-gegevens helpen bij het

identificeren van personen, terwijl PNR-gegevens geen identificatiedoel hebben maar de details ervan bijdragen tot het uitvoeren van risicobeoordelingen van personen, het verkrijgen van inlichtingen en het leggen van verbanden tussen bekende en onbekende personen.

15. Het doel van de beoogde maatregelen bestrijkt niet alleen het arresteren van bekende personen, maar ook het lokaliseren van personen die onder de criteria van het voorstel kunnen vallen.

Om die personen te identificeren, staan risicoanalyse en de vaststelling van patronen centraal in het project. In overweging 9 van het voorstel staat uitdrukkelijk dat de gegevens „voldoende lang” moeten „worden bewaard om risico-indicatoren te ontwikkelen en reis- en gedragspatronen te kunnen afleiden”.

16. Het doel wordt aldus op twee niveaus beschreven: het eerste niveau is de algemene doelstelling om terrorisme en georganiseerde criminaliteit te bestrijden, terwijl het tweede niveau de middelen en maatregelen omvat die inherent zijn aan de verwezenlijking van deze doelstelling. Hoewel bestrijding van terrorisme en georganiseerde criminaliteit als doel duidelijk genoeg en rechtmatig lijkt te zijn, zijn de middelen om dit doel te bereiken voor discussie vatbaar.

Afleiden van patronen en risicobeoordeling

17. Het voorstel geeft geen indicatie over de manier waarop patronen zullen worden afgeleid en de risicobeoordeling zal worden verricht. De effectbeoordeling bevat de volgende verduidelijking met betrekking tot de manier waarop PNR-gegevens zullen worden gebruikt: vergelijking van PNR-gegevens „met een combinatie van kenmerken en gedragspatronen, teneinde een risicobeoordeling te maken. Wanneer een passagier binnen een bepaalde risicobeoordeling past, kan hij worden geïdentificeerd als een passagier met een hoog risico” ⁽³⁾.
18. Verdachte personen zouden kunnen worden geselecteerd op basis van concrete elementen van verdenking in hun PNR-gegevens (bv. contact met een verdacht reisagentschap, referentie van een gestolen creditcard) alsook van „patronen” of een abstract profiel. Op basis van reispatronen kunnen namelijk verschillende standaardprofielen worden opgesteld voor „normale passagiers” en voor „verdachte passagiers”. Met deze profielen zouden de passagiers die niet onder de categorie „normale passagiers” vallen verder kunnen worden onderzocht, vooral indien hun profiel wordt geassocieerd met andere elementen van verdenking, zoals een gestolen creditcard.
19. Hoewel niet kan worden aangenomen dat passagiers in het vizier komen op grond van hun godsdienst of andere gevoelige gegevens, blijkt niettemin dat zij voor onderzoek in aanmerking zouden komen op basis van een mix van concrete en abstracte informatie, waaronder standaardpatronen en abstracte profielen.

⁽¹⁾ Verdrag van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, 28 januari 1981.

⁽²⁾ Toelichting bij het voorstel, punt 1.

⁽³⁾ Effectbeoordeling, punt 2.1, „Beschrijving van het probleem”.

20. Er valt over te discussiëren of dit soort onderzoek profilering kan worden genoemd. Profilering zou bestaan in een computermethode die, door datamining toe te passen op een datawarehouse, de indeling, met een bepaalde waarschijnlijkheid — en dus met een bepaalde foutenmarge — van een persoon in een specifieke categorie mogelijk maakt of moet maken, zodat ten aanzien van die persoon individuele beslissingen kunnen worden genomen ⁽¹⁾.
21. De EDPS weet dat er discussies over de definitie van profilering aan de gang zijn. Of nu al dan niet officieel wordt erkend dat het voorstel strekt tot *het profileren* van passagiers, het belangrijkste punt waar het hier om gaat heeft geen betrekking op definities, maar op het effect op personen.
22. De bezorgdheid van de EDPS is vooral dat beslissingen over individuen zullen worden genomen op basis van patronen en criteria die zijn vastgesteld met gebruikmaking van de gegevens van passagiers in het algemeen. Aldus kunnen over één bepaalde persoon beslissingen worden genomen op basis (tenminste gedeeltelijk) van patronen die uit de gegevens van *andere* personen zijn afgeleid. Dus zullen in verhouding tot een abstracte context beslissingen worden genomen die zeer ingrijpend kunnen zijn voor de betrokkenen. Het is voor individuele personen uiterst moeilijk zich tegen dergelijke beslissingen te verdedigen.
23. Voorts moet de risicobeoordeling worden verricht zonder dat er eenvormige normen voor de identificatie van verdachte personen zijn. De EDPS heeft ernstige vragen bij de rechtszekerheid van het volledige filterproces, aangezien de criteria op basis waarvan iedere passagier zal worden doorgelicht zo slecht gedefinieerd zijn.
24. De EDPS herinnert aan de jurisprudentie van het Europees Hof voor de Rechten van de Mens, volgens dewelke het nationale recht voldoende precies moet zijn om de burgers aan te geven in welke omstandigheden en op welke voorwaarden de overheid gemachtigd is om informatie over

hun privé-leven op te slaan en te gebruiken. De informatie „moet toegankelijk zijn voor de betrokkene en qua gevolgen voorzienbaar zijn”. Een voorschrift is „voorzienbaar” indien het „voldoende nauwkeurig” is om iedere persoon — zonodig met deskundig advies — in staat te stellen „zijn gedrag daarop af te stemmen” ⁽²⁾.

25. Ten slotte moet het onderhavige voorstel omwille van dit soort risico's aandachtig worden bestudeerd. Hoewel het algemene doel van bestrijding van terrorisme en georganiseerde misdaad op zich duidelijk en rechtmatig is, blijkt de essentie van de te verrichten verwerking niet voldoende omschreven en verantwoord te zijn. De EDPS dringt er derhalve bij de EU-wetgever op aan dit helder te krijgen voordat het kaderbesluit wordt aangenomen.

Noodzakelijkheid

26. Het inbreuk makende karakter van de maatregelen is duidelijk, zoals hierboven is aangetoond. Anderzijds is het nut verre van aangetoond.
27. De effectbeoordeling betreffende het voorstel is eerder toegespitst op de beste manier om EU-PNR vast te stellen, dan op de noodzaak van die PNR. In de effectbeoordeling ⁽³⁾ wordt verwezen naar PNR-systemen in andere landen, namelijk in de Verenigde Staten en het Verenigd Koninkrijk. Het gebrek aan precieze gegevens en cijfers over deze systemen valt evenwel te betreuren. In het Britse seinsysteem wordt melding gemaakt van „talrijke arrestaties” met betrekking tot „verscheidene misdrijven”, zonder dat enige precisering over het verband met terrorisme of georganiseerde criminaliteit wordt gegeven. Er worden geen details verstrekt over het programma van de Verenigde Staten, behalve dat „de EU de waarde van PNR-gegevens heeft kunnen vaststellen en zich bewust geworden is van het potentieel hiervan voor wetshandhavingsdoelinden”.
28. Niet alleen is er in het voorstel een gebrek aan precieze informatie over de concrete resultaten van die PNR-systemen, maar evenmin wordt de doeltreffendheid van de maatregelen in dit stadium bevestigd door verslagen die *door andere instanties*, zoals de GAO in de Verenigde Staten, zijn gepubliceerd ⁽⁴⁾.

⁽¹⁾ Deze definitie komt uit een recente studie over profilering van de Raad van Europa: *L'application de la Convention 108 au mécanisme de profilage, Éléments de réflexion destinés au travail futur du Comité consultatif (T-PD)*, Jean-Marc Dinant, Christophe Lazaro, Yves Pouillet, Nathalie Lefever, Antoinette Rouvroy, november 2007 (nog niet gepubliceerd). Zie ook de definitie van Lee Bygrave: „Generally speaking, profiling is the process of inferring a set of characteristics (typically behavioural) about an individual person or collective entity and then treating that person/entity (or other persons/entities) in the light of these characteristics. As such, the profiling process has two main components: i) profile generation — the process of inferring a profile; ii) profile application — the process of treating persons/entities in light of this profile”. L. A. BYGRAVE, *Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, *Computer Law & Security Report*, 2001, vol. 17, pp. 17-24: <http://www.austlii.edu.au/au/journals/PLPR/2000/40.html>

⁽²⁾ Rotaru tegen Roemenië, nr. 28341/95, §§ 50, 52 en 55.

Zie ook Amann tegen Zwitserland, nr. 27798/95, §§ 50 en volgende.

⁽³⁾ Punt 2.1, „Beschrijving van het probleem”.

⁽⁴⁾ Zie bijvoorbeeld het verslag van de *Government Accountability Office* van de Verenigde Staten aan verzoekers in het Congres van mei 2007, „*Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues remain*”: <http://www.gao.gov/new.items/d07346.pdf>

29. De EDPS is van oordeel dat technieken die erin bestaan het door bepaalde personen gevormde risico te beoordelen door middel van datamininginstrumenten en gedragspatronen, verder moeten worden geëvalueerd, en dat het nut ervan duidelijk moet worden vastgesteld in het kader van de terrorismebestrijding, alvorens zij op zo'n grote schaal worden gebruikt.

Evenredigheid

30. Om de balans tussen de inbreuk op de privacy van de persoon en de noodzakelijkheid van de maatregel te beoordelen ⁽¹⁾, wordt rekening gehouden met de volgende elementen:

- de maatregelen gelden voor alle passagiers, ongeacht of een onderzoek naar hen is ingesteld door wetshandhavingsautoriteiten. Het gaat om proactief onderzoek, op nooit eerder geziene schaal;
- besluiten over personen kunnen gebaseerd zijn op abstracte profielen, die dus een aanzienlijke foutenmarge omvatten;
- de aard van de maatregelen die ten aanzien van de persoon moeten worden genomen, houdt verband met de wetshandhaving: de gevolgen qua uitsluiting of dwang vormen daarom een veel grotere inbreuk dan in andere contexten, zoals fraude met creditcards of marketing.

31. Het evenredigheidsbeginsel respecteren houdt niet alleen in dat de voorgestelde maatregel doeltreffend is, maar ook dat het met het voorstel beoogde doel niet kan worden bereikt met instrumenten die minder inbreuk maken op de privacy. De doeltreffendheid van de beoogde maatregelen is niet aangetoond. Het bestaan van alternatieven moet zorgvuldig worden geëvalueerd alvorens aanvullende/nieuwe maatregelen worden vastgesteld voor het verwerken van persoonsgegevens. Volgens de EDPS heeft deze alomvattende evaluatie niet plaatsgevonden.

32. De EDPS wenst te herinneren aan de andere grootschalige systemen voor toezicht op de bewegingen van personen binnen of aan de grenzen van de EU, die in werking zijn of weldra in werking zullen worden gesteld, waaronder met name het Visuminformatiesysteem ⁽²⁾ en het Schengeninformatiesysteem ⁽³⁾. Hoewel deze instrumenten de

bestrijding van terrorisme of georganiseerde criminaliteit niet als voornaamste doel hebben, zijn zij in zekere mate toegankelijk voor wetshandhavingsinstanties — of zullen zij dat worden — voor het ruimere toepassingsgebied van de criminaliteitsbestrijding ⁽⁴⁾.

33. Een ander voorbeeld heeft betrekking op de beschikbaarheid van persoonsgegevens die in nationale politiedatabanken zijn opgeslagen — voornamelijk in verband met biometrische gegevens — in het kader van het in mei 2005 ondertekende Verdrag van Prüm, dat tot alle lidstaten van de Europese Unie wordt uitgebreid ⁽⁵⁾.

34. Deze verschillende instrumenten hebben met elkaar gemeen dat zij een algemeen toezicht op de bewegingen van personen mogelijk maken, zij het vanuit verschillende perspectieven. De manier waarop zij reeds kunnen bijdragen tot de bestrijding van specifieke criminaliteitsvormen, met inbegrip van terrorisme, moet grondig en uitvoerig worden onderzocht vooraleer wordt besloten een nieuwe vorm van systematische doorlichting van alle personen die de EU per vliegtuig verlaten of binnenkomen, vast te stellen. De EDPS beveelt aan dat de Commissie een dergelijk onderzoek zou voeren, als een noodzakelijke stap in de wetgevingsprocedure.

Conclusie

35. In het licht van het bovenstaande concludeert de EDPS het volgende met betrekking tot de rechtmatigheid van de voorgestelde maatregelen. Voortbouwen op verschillende databanken zonder algemeen zicht op de concrete resultaten en tekortkomingen:

- is in strijd met een rationeel wetgevingsbeleid; waarin nieuwe instrumenten niet mogen worden aangenomen voordat de bestaande volledig uitgevoerd zijn en onvoldoende gebleken zijn ⁽⁶⁾;
- kan er toe leiden dat wij evolueren naar een totaal gecontroleerde samenleving.

36. Terrorismebestrijding kan zeker een legitieme grond zijn om uitzonderingen op de fundamentele rechten op privacy en gegevensbescherming te hanteren. Om geldig te zijn echter moet de noodzakelijkheid van de inbreuk met

⁽¹⁾ Volgens artikel 9 van Verdrag nr. 108 „kan van het in de artikelen 5, 6 en 8 van dit Verdrag bepaalde worden afgeweken, indien de wet van de Partij in een dergelijke afwijking voorziet en het hier een maatregel betreft die in een democratische samenleving noodzakelijk is ten behoeve van:

1. de bescherming van de veiligheid van de staat, de openbare veiligheid, de geldelijke belangen van de staat of de bestrijding van strafbare feiten;
2. de bescherming van de betrokkene en van de rechten en vrijheden van anderen.”

⁽²⁾ Beschikking 2004/512/EG van de Raad van 8 juni 2004 betreffende het opzetten van het Visuminformatiesysteem (VIS) (PB L 213 van 15.6.2004, blz. 5); voorstel voor een verordening van het Europees Parlement en de Raad betreffende het visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van informatie op het gebied van visa voor kort verblijf, COM(2004) 835 def. Zie het voorstel voor een besluit van de Raad over de toegang tot het visuminformatiesysteem (VIS) voor raadpleging door de nationale veiligheidsdiensten van de lidstaten en Europol, met het oog op het voorkomen, opsporen en onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten, COM(2005) 600 def.

⁽³⁾ Zie met name Besluit 2007/533/JBZ van de Raad van 12 juni 2007 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) (PB L 205 van 7.8.2007).

⁽⁴⁾ Zie in dit verband: Advies van de Europese Toezichthouder voor gegevensbescherming over het voorstel voor een besluit van de Raad over de toegang tot het visuminformatiesysteem (VIS) voor raadpleging door de nationale veiligheidsdiensten van de lidstaten en Europol, met het oog op het voorkomen, opsporen en onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten (COM(2005) 600 def.) (PB C 97 van 25.4.2006, blz. 6).

⁽⁵⁾ Zie de adviezen van de EDPS over de besluiten betreffende het Verdrag van Prüm: Advies van 4 april 2007 betreffende het initiatief van 15 lidstaten met het oog op de aanneming van een besluit van de Raad inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit (PB C 169 van 21.7.2007, blz. 2) en Advies van 19 december 2007 over het initiatief van de Bondsrepubliek Duitsland met het oog op de aanneming van een besluit van de Raad betreffende de uitvoering van Besluit 2007/.../JBZ inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit, beschikbaar op: <http://www.edps.europa.eu>

⁽⁶⁾ De EDPS heeft dit punt al verscheidene keren gemaakt, zeer recent nog in zijn advies van 25 juli 2007 over de toepassing van de richtlijn gegevensbescherming (PB C 255 van 27.10.2007, blz. 1).

duidelijke en onweerlegbare elementen worden ondersteund, en moet de evenredigheid van de verwerking worden aangetoond. Dit geldt des te meer bij een grote inbreuk op de persoonlijke levenssfeer zoals dit voorstel beoogt.

37. Er kan alleen worden opgemerkt dat dergelijke verantwoordingselementen in het voorstel ontbreken en dat het de noodzakelijkheids- en de evenredigheidstoets niet kan doorstaan.
38. De EDPS benadrukt het essentiële karakter van de bovengenoemde noodzakelijkheids- en evenredigheidstoets. Deze vormt een *conditio sine qua non* voor de inwerkingtreding van het onderhavige voorstel. Verdere opmerkingen van de EDPS in dit advies moeten in het licht van deze voorafgaande voorwaarde worden gezien.

III. TOEPASSELIJK RECHT — UITOEFENING VAN DE RECHTEN VAN DE BETROKKENE

Toepasselijk recht

39. De onderstaande analyse is toegespitst op drie punten:
- een beschrijving van de verschillende fasen van de verwerking waarin het voorstel voorziet, met het oog op bepaling van het recht dat in ieder stadium van toepassing is;
 - de beperkingen van het voorstel voor een kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politieke en justitiële samenwerking in strafzaken wat het toepassingsgebied en de rechten van de betrokkene betreft;
 - een meer algemene analyse van de mate waarin een derdepijlerinstrument kan gelden voor particuliere actoren die in een eerste pijlerkader gegevens verwerken.

Het toepasselijk recht in de verschillende fasen van de verwerking

40. In artikel 11 van het voorstel staat: „De lidstaten zorgen ervoor dat het Kaderbesluit (...) van de Raad inzake de bescherming van persoonsgegevens die worden verwerkt in het kader van de politieke en justitiële samenwerking in strafzaken van toepassing is op de verwerking van persoonsgegevens krachtens dit kaderbesluit.”
41. Ondanks deze bepaling is het evenwel niet duidelijk in welke mate het kaderbesluit gegevensbescherming — een instrument van de derde pijler van het EU-Verdrag — van toepassing zal zijn op door luchtvaartmaatschappijen verwerkte, door PIU's verzamelde en door andere bevoegde autoriteiten verder gebruikte gegevens.
42. De eerste fase in de verwerking van persoonsgegevens waarin het voorstel voorziet, is de verwerking door luchtvaartmaatschappijen, die verplicht zijn PNR-gegevens —

in principe via de „pushmethode” — beschikbaar te stellen aan nationale PIU's. Uit de formulering van het voorstel en de effectbeoordeling ⁽¹⁾ zou men kunnen opmaken dat de luchtvaartmaatschappijen de gegevens ook als bulkdata aan intermediairs kunnen overdragen. Luchtvaartmaatschappijen zijn voornamelijk actief in een commerciële omgeving, waarvoor de nationale wetgeving inzake gegevensbescherming tot uitvoering van Richtlijn 95/46/EG geldt ⁽²⁾. Wanneer de verzamelde gegevens voor wetshandhavingsdoelinden worden gebruikt, zullen er vragen over het toepasselijke recht rijzen ⁽³⁾.

43. De gegevens zouden vervolgens door een intermediair worden gefilterd (om te worden geformatteerd en om PNR-gegevens uit te sluiten die niet op de lijst van de in het voorstel vereiste gegevens staan) of rechtstreeks aan de PIU's worden toegezonden. Intermediairs kunnen ook actoren uit de particuliere sector zijn, zoals SITA, een bedrijf dat in die zin actief is in het kader van de PNR-Overeenkomst met Canada.

44. Wat de PIU's betreft, die verantwoordelijk zijn voor de risicobeoordeling van alle gegevens, is het niet duidelijk wie verantwoordelijk zal zijn voor de verwerking. Het is mogelijk dat de douane- en grensautoriteiten erbij worden betrokken, en niet noodzakelijkerwijs de wetshandhavingsautoriteiten.

45. De daaropvolgende doorgifte van gefilterde gegevens aan de „bevoegde” autoriteiten zou waarschijnlijk in een wetshandhavingscontext geschieden. In het voorstel is bepaald dat „bevoegde autoriteiten uitsluitend autoriteiten kunnen zijn die verantwoordelijk zijn voor de voorkoming en bestrijding van terroristische misdrijven en georganiseerde criminaliteit”.

46. Naarmate de verwerking vordert, houden de betrokken actoren en het nagestreefde doel meer verband met de politieke en justitiële samenwerking in strafzaken. In het voorstel wordt evenwel niet uitdrukkelijk vermeld op welk moment precies het kaderbesluit gegevensbescherming van toepassing wordt. Afgaand op de formulering zou zelfs kunnen worden gedacht dat het op de volledige verwerking van toepassing is, en zelfs op de luchtvaartmaatschappijen ⁽⁴⁾. Het kaderbesluit gegevensbescherming houdt echter op zich een aantal beperkingen in.

⁽¹⁾ Artikel 6, lid 3, van het voorstel en Effectbeoordeling, bijlage A, Methode voor de overdracht van gegevens door de luchtvervoerders.

⁽²⁾ 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 (PB L 281 van 23.11.1995, blz. 31).

⁽³⁾ Zie in dit verband de gevolgen van het PNR-arrest. Arrest van het Hof van 30 mei 2006 in de gevoegde zaken C-317/04, Parlement tegen Raad, en C-318/04, Parlement tegen Commissie, Jurispr. 2006, punt 56.

⁽⁴⁾ Artikel 11 van het voorstel: Zie ook overweging 10 in de preambule: „Het Kaderbesluit (...) van de Raad inzake de bescherming van persoonsgegevens die worden verwerkt in het kader van de politieke en justitiële samenwerking in strafzaken moet van toepassing zijn op alle gegevens die in overeenstemming met dit kaderbesluit worden verwerkt. De rechten van de betrokkenen bij dergelijke verwerking, zoals het recht in kennis te worden gesteld, het recht op toegang en het recht om gegevens te laten corrigeren, wissen of afschermen, evenals het recht op schadeloosstelling en het aanwenden van rechtsmiddelen zijn zoals vastgelegd in dat kaderbesluit.”

47. In dit verband betwijfelt de EDPS fundamenteel of titel VI van het EU-Verdrag als rechtsgrondslag kan dienen om wettelijke verplichtingen op routinematige basis voor wetshandavingsdoeleinden op te leggen aan actoren uit de particuliere sector. Voorts is de vraag relevant of titel VI van het EU-Verdrag als rechtsgrondslag kan dienen om wettelijke verplichtingen op te leggen aan overheidsinstellingen die in principe buiten het kader van de samenwerking op het gebied van wetshandhaving staan. Deze vragen zullen verder op in dit advies worden behandeld.

Beperkingen van het kaderbesluit gegevensbescherming

48. De tekst van het voorstel voor een kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politieke en justitiële samenwerking in strafzaken bevat ten minste twee beperkingen die van belang zijn wat het toepassingsgebied betreft.

49. In de eerste plaats wordt het toepassingsgebied van het kaderbesluit gegevensbescherming duidelijk omschreven in het kaderbesluit zelf: het „is alleen van toepassing op gegevens die door de bevoegde autoriteiten worden verzameld of verwerkt met het oog op preventie, onderzoek, opsporing en vervolging ter zake van strafbare feiten en tenuitvoerlegging van straffen” ⁽¹⁾.

50. In de tweede plaats wordt het kaderbesluit gegevensbescherming niet geacht van toepassing te zijn op gegevens die louter op nationaal niveau worden verwerkt, maar is het beperkt tot gegevens die tussen de lidstaten worden uitgewisseld en de verdere doorgifte aan derde landen ⁽²⁾.

51. Het kaderbesluit gegevensbescherming bevat ook een aantal nadelen in vergelijking met Richtlijn 95/46/EG, met name een ruime uitzondering op het doelbeperkingsbeginsel. Met betrekking tot dit beginsel beperkt het voorstel het doel van de verwerking duidelijk tot de bestrijding van terrorisme en georganiseerde criminaliteit. Het kaderbesluit gegevensbescherming laat evenwel verwerking voor ruimere doeleinden toe. In een dergelijk geval moet de *lex specialis* (het voorstel) prevaleren boven de *lex generalis* (het kaderbesluit gegevensbescherming) ⁽³⁾. Dit moet uitdrukkelijk worden gesteld in de tekst van het voorstel.

52. Daarom beveelt de EDPS aan de volgende bepaling aan het voorstel toe te voegen: „Persoonsgegevens die overeenkomstig dit kaderbesluit door luchtvaartmaatschappijen worden overgedragen, mogen niet voor andere doeleinden dan de bestrijding van terrorisme en georganiseerde criminaliteit worden verwerkt. De uitzonderingen op het doelbeginsel waarin is voorzien in het kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politieke en justitiële samenwerking in strafzaken, gelden niet.”.

⁽¹⁾ Overweging 5 bis, versie van 11 december 2007 van het kaderbesluit gegevensbescherming.

⁽²⁾ Artikel 1.

⁽³⁾ In verband met dit punt moet de tekst van artikel 27 *ter* van de laatste versie van het kaderbesluit over gegevensbescherming in de derde pijler zorgvuldig worden bestudeerd en besproken.

53. Concluderend neemt de EDPS nota van een ernstig gebrek aan rechtszekerheid met betrekking tot de gegevensbeschermingsregeling die van toepassing is op de verschillende bij het project betrokken actoren, met name luchtvaartmaatschappijen en andere actoren uit de eerste pijler: of dit nu de regels van het voorstel, de regels van het kaderbesluit gegevensbescherming of de nationale wetgeving ter uitvoering van Richtlijn 95/46/EG zijn. De wetgever moet duidelijk maken op welk ogenblik van de verwerking deze verschillende regels precies zullen gelden.

Voorwaarden voor de toepassing van de regels van de eerste en de derde pijler

54. De EDPS heeft fundamentele vragen bij het feit dat een instrument van de derde pijler routinematige wettelijke verplichtingen voor wetshandavingsdoeleinden schept voor actoren uit de particuliere of de publieke sector die in principe buiten het kader van de samenwerking op wetshandavingsgebied staan.

55. Hier kan een vergelijking worden gemaakt met twee andere gevallen waarin de particuliere sector werd betrokken bij de bewaring of doorgifte van gegevens met het oog op wetshandaving:

— *de PNR-overeenkomst met de Verenigde Staten waarbij in een systematische doorgifte van PNR-gegevens door luchtvaartmaatschappijen aan wetshandavingsinstanties was voorzien*. Het arrest van het Hof van Justitie in de PNR-zaak heeft uitgesloten dat de Gemeenschap bevoegd zou zijn om de PNR-overeenkomst te sluiten. Een van de redenen daarvoor was dat de doorgifte van de PNR-gegevens aan het CBP van de Verenigde Staten een verwerking is die betrekking heeft op de openbare veiligheid en de activiteiten van de staat op strafrechtelijk gebied ⁽⁴⁾. In dit geval was de verwerking een *systematische* doorgifte aan het CBP, waarin het verschilt van het volgende geval;

— *de algemene bewaring van gegevens door operatoren van elektronische communicatie*. Met betrekking tot de Gemeenschapsbevoegdheid om een dergelijke bewaringstermijn vast te stellen, kan een verschil met het geval van de VS-PNR worden gemaakt, aangezien Richtlijn 2006/24/EG ⁽⁵⁾ alleen in een verplichting tot bewaring voorziet, waarbij de gegevens onder het beheer van de operatoren blijven. Er wordt geen systematische doorgifte van gegevens aan wetshandavingsautoriteiten beoogd. Er kan worden geconcludeerd dat, voor zover de gegevens onder het beheer van de dienstverleners blijven, deze aanbidders ten aanzien van de betrokkene ook verantwoordelijk blijven voor de nakoming van de verplichtingen in verband met de bescherming van persoonsgegevens.

⁽⁴⁾ Arrest van het Hof van 30 mei 2006 in de gevoegde zaken C-317/04, Parlement tegen Raad, en C-318/04, Parlement tegen Commissie, Jurispr. 2006, punt 56.

⁽⁵⁾ Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (PB L 105 van 13.4.2006, blz. 54).

56. In het onderhavige voorstel betreffende EU-PNR moeten de luchtvaartmaatschappijen de PNR-gegevens van alle passagiers systematisch beschikbaar stellen. Deze gegevens worden evenwel niet rechtstreeks als bulkdata doorgegeven aan wetshandavingsinstanties: ze kunnen aan een intermediair worden gezonden en ze worden geëvalueerd door een derde partij waarvan het statuut onduidelijk blijft, alvorens de geselecteerde informatie aan de bevoegde autoriteiten wordt gezonden.

57. Het grootste deel van de verwerking gebeurt in een grijze zone die zowel met de eerste als met de derde pijler materieel verband houdt. Zoals in deel IV zal worden besproken, is de hoedanigheid van de actoren die de gegevens verwerken niet duidelijk. Luchtvaartmaatschappijen zijn duidelijk geen handavingsautoriteiten, en intermediairs kunnen actoren uit de particuliere sector zijn. Zelfs met betrekking tot PIU's die publieke overheden zouden zijn, moet worden benadrukt dat niet iedere overheidsinstelling over de hoedanigheid en de bevoegdheden beschikt om op routinebasis wetshandavingstaken te vervullen.

58. Van oudsher is er een duidelijke scheiding tussen wetshandhaving en activiteiten van de particuliere sector, waarbij wetshandavingstaken door speciaal daarvoor bevoegde autoriteiten, met name de politiediensten, worden vervuld en particuliere actoren per geval wordt verzocht om persoonsgegevens te verstrekken aan deze handavingsautoriteiten. Er is nu een tendens om systematisch samenwerking voor wetshandavingsdoeleinden op te leggen aan particuliere actoren, hetgeen de vraag doet rijzen welk gegevensbeschermingskader (eerste of derde pijler) van toepassing is op de voorwaarden van deze samenwerking: moeten de regels op de hoedanigheid van de verantwoordelijke voor de verwerking (particuliere sector) of op het beoogde doel (wetshandhaving) worden gebaseerd?

59. De EDPS heeft reeds gewezen op het risico van een juridisch vacuüm tussen activiteiten in de eerste en de derde pijler⁽¹⁾. Het is inderdaad verre van duidelijk of activiteiten van particuliere bedrijven die in zekere zin verband houden met de wetshandhaving op strafrechtelijk gebied tot het werkterrein van de wetgever van de Europese Unie op grond van de artikelen 30, 31 en 34 EU-Verdrag behoren.

60. Indien het algemene (eerste pijler-) kader niet van toepassing is, zouden dienstverleners moeilijke onderscheiden moeten maken in hun gegevensbanken. Onder de huidige regeling is het duidelijk dat de verantwoordelijke voor de verwerking ten aanzien van de betrokkenen dezelfde mate van gegevensbescherming in acht moet nemen, ongeacht de doeleinden die de bewaring van de gegevens rechtvaardigen. Daarom moet vermeden worden dat verwerking door dienstverleners voor verschillende doeleinden aan verschillende kaders voor gegevensbescherming zou worden onderworpen.

⁽¹⁾ Zie het Advies van de Europese Toezichthouder voor gegevensbescherming inzake de mededeling van de Commissie aan het Europees Parlement en de Raad over de follow-up van het werkprogramma voor een betere toepassing van de richtlijn gegevensbescherming (PB C 255 van 27.10.2007, blz. 1). Zie ook het Jaarverslag 2006, blz. 47.

Uitoefening van de rechten van de betrokkene

61. Indien verschillende wettelijke regelingen op nationaal niveau van toepassing zijn, zou dit voornamelijk een groot effect hebben op de uitoefening door de betrokkene van zijn rechten.

62. In de preambule van het voorstel staat dat „het recht in kennis te worden gesteld, het recht op toegang en het recht om gegevens te laten corrigeren, wissen of afschermen, evenals het recht op schadeloosstelling en het aanwenden van rechtsmiddelen zijn zoals vastgelegd” in het kaderbesluit gegevensbescherming. Met deze verklaring wordt echter geen antwoord gegeven op de vraag wie de verantwoordelijke voor de verwerking is die verzoeken van betrokkenen moet beantwoorden.

63. De informatie over de verwerking zou door luchtvaartmaatschappijen kunnen worden verstrekt, maar de kwestie is complexer wanneer het over toegang tot of correctie van gegevens gaat. Deze rechten zijn immers beperkt op grond van het kaderbesluit gegevensbescherming. Zoals hierboven is gezegd, valt te betwijfelen of een dienstverlener zoals een luchtvaartmaatschappij kan worden verplicht om, afhankelijk van het beoogde doel (commercieel of wetshandhaving), gedifferentieerde rechten op toegang tot en correctie van de door hem bijgehouden gegevens te verlenen. Er kan worden aangevoerd dat deze rechten voor de PIU of de anderszins aangewezen bevoegde autoriteiten moeten worden uitgeoefend. Het voorstel geeft evenwel geen verdere indicatie in dit verband, en zoals reeds is vermeld, is het ook niet duidelijk of deze autoriteiten (tenminste de PIU's) wetshandavingsinstanties zullen zijn die normaliter met beperkte (evt. indirecte) toegangsprocedures worden belast.

64. Wat de PIU's betreft, dreigt de betrokkene ook met verschillende ontvangers van de gegevens te worden geconfronteerd; de gegevens worden nl. overgedragen aan de PIU van het land van vertrek/aankomst van de vluchten, maar per geval mogelijk ook aan PIU's van andere lidstaten. Bovendien is het mogelijk dat verschillende lidstaten één gemeenschappelijke PIU willen oprichten of aanwijzen. In dat geval moet de betrokkene zijn verhaalrecht misschien voor een autoriteit van een andere lidstaat uitoefenen. Ook hier is het niet duidelijk of de nationale regels inzake gegevensbescherming van toepassing zullen zijn (deze worden geacht geharmoniseerd te zijn binnen de EU), dan wel of rekening moet worden gehouden met specifieke wetgeving inzake wetshandhaving (gezien het gebrek aan algemene harmonisatie in de derde pijler op nationaal niveau).

65. Dezelfde vraag rijst in verband met de toegang tot gegevens die worden verwerkt door intermediairs, waarvan de status onduidelijk is, en die ook dezelfde zouden kunnen zijn voor luchtvaartmaatschappijen in verschillende landen van de EU.

66. De EDPS betreurt de onzekerheid die blijft bestaan met betrekking tot de uitoefening van deze fundamentele rechten van de betrokkene. Hij benadrukt dat deze situatie grotendeels te wijten is aan het feit dat actoren die wets-handhaving niet als hoofdpodracht hebben, met dergelijke taken worden belast.

Conclusie

67. De EDPS is van oordeel dat in het voorstel duidelijk moet worden gemaakt welke wettelijke regeling van toepassing is in welk stadium van de verwerking, en dat moet worden gespecificeerd jegens welke actor of autoriteit het recht op toegang en verhaal moet worden uitgeoefend. De EDPS herinnert eraan dat bepalingen betreffende gegevensbescherming overeenkomstig artikel 30, lid 1, onder b), van het EU-Verdrag passend moeten zijn en het volledige scala van in het voorstel vastgestelde verwerkingen moeten bestrijken. Een eenvoudige verwijzing naar het kaderbesluit gegevensbescherming volstaat niet, gezien het beperkte toepassingsgebied van dat kaderbesluit en de erin vervatte beperking van rechten. Voor zover het om wets-handhavingsautoriteiten gaat, moeten de regels van het kaderbesluit gegevensbescherming ten minste van toepassing zijn op de volledige verwerking waarin het voorstel voorziet, teneinde de coherentie van de toepassing van de gegevensbeschermingsbeginselen te garanderen.

IV. HOEDANIGHEID VAN DE ONTVANGERS

68. De EDPS neemt er nota van dat het voorstel niet in specificaties voorziet met betrekking tot de hoedanigheid van de ontvangers van door luchtvaartmaatschappijen verzamelde persoonsgegevens, hetzij intermediairs, passagiersinformatie-eenheden of bevoegde autoriteiten. Er moet worden benadrukt dat de hoedanigheid van de ontvanger rechtstreeks verband houdt met het soort garanties inzake gegevensbescherming die voor die ontvanger gelden. Het verschil tussen de garanties waarin met name door de regels van de eerste en de derde pijler is voorzien, is reeds vermeld. Het is van essentieel belang dat de toepasselijke regeling duidelijk is voor alle betrokken actoren, waaronder de nationale regeringen, de wetshandhavingsinstanties, de gegevensbeschermingsautoriteiten, alsook de verantwoordelijken voor de verwerking en de betrokkenen.

Intermediairs

69. In het voorstel wordt geen indicatie gegeven met betrekking tot de hoedanigheid van intermediairs⁽¹⁾. De rol van intermediairs als verantwoordelijken voor de verwerking of als verwerkers is evenmin gespecificeerd. De ervaring leert dat een entiteit uit de particuliere sector — een computerboekingsysteem of een andere entiteit — perfect kan worden belast met de taak om rechtstreeks PNR-gegevens te verzamelen bij luchtvaartmaatschappijen om ze vervolgens door te geven aan PIU's. Dat is namelijk de manier waarop gegevens worden verwerkt in het kader

van de PNR-Overeenkomst met Canada. SITA⁽²⁾ is het bedrijf dat verantwoordelijk is voor de verwerking van de informatie. De rol van de intermediair is van doorslaggevend belang, aangezien hij verantwoordelijk kan zijn voor het uitfilteren/herformatteren van door luchtvaartmaatschappijen in onverwerkte vorm overgedragen gegevens⁽³⁾. Ook al zijn de intermediairs verplicht om de verwerkte informatie te wissen zodra deze aan de PIU's is doorgegeven, de verwerking op zich is hoogst gevoelig: een gevolg van het optreden van intermediairs is dat een extra databank wordt aangelegd die enorme hoeveelheden gegevens bevat, en zelfs, volgens het voorstel, gevoelige gegevens (in dat geval zijn de intermediairs verplicht die gevoelige gegevens te wissen). Daarom beveelt de EDPS aan geen intermediairs bij de verwerking van passagiersgegevens te betrekken, tenzij hun hoedanigheid en taken duidelijk gespecificeerd zijn.

Passagiersinformatie-eenheden

70. PIU's hebben een beslissende rol bij het identificeren van personen die bij terrorisme of georganiseerde criminaliteit betrokken (kunnen) zijn of ermee geassocieerd (kunnen) worden. Volgens het voorstel zullen zij verantwoordelijk zijn voor het ontwikkelen van risico-indicatoren en het verstrekken van inlichtingen over reispatronen⁽⁴⁾. Wanneer de risicobeoordeling op gestandaardiseerde reispatronen gebaseerd is en niet op bewijsmateriaal in verband met een concreet geval, kan de analyse als proactief onderzoek worden beschouwd. De EDPS benadrukt dat dit soort verwerking in principe strikt geregeld (zo niet verboden) is in de wetgeving van de lidstaten, en de taak is van specifieke overheidsinstellingen waarvan de werking ook strikt is geregeld.
71. Aan de PIU's wordt daarom de zeer gevoelige verwerking van informatie toevertrouwd, maar het voorstel geeft geen bijzonderheden over hun hoedanigheid en over de voorwaarden waaronder zij deze taak zouden uitoefenen. Hoewel het waarschijnlijk is dat deze door een regeringsinstantie, mogelijk de douane of een grenscontrole-dienst, zal worden verricht, verbiedt het voorstel de lidstaten niet uitdrukkelijk om deze taak aan inlichtingendiensten of zelfs om het even welke verwerker toe te vertrouwen. De EDPS onderstreept dat de transparantie en de garanties die voor inlichtingendiensten gelden, niet altijd dezelfde zijn als die welke voor de traditionele wets-handhavingsautoriteiten gelden. Nadere gegevens over de hoedanigheid van de PIU's zijn van doorslaggevend belang, aangezien dit rechtstreekse gevolgen zal hebben voor het toepasselijke rechtskader en de voorwaarden voor toezicht. De EDPS is van oordeel dat het voorstel een aanvullende bepaling moet bevatten waarin de specifieke kenmerken van de PIU's worden genoemd.

⁽²⁾ SITA is in 1949 opgericht door 11 luchtvaartmaatschappijen. Oplossingen met een meerwaarde worden aan de luchtvervoersector verstrekt via het commerciële bedrijf SITA INC (*Information, Networking Computing*) en netwerkdiensten via SITA SC op coöperatieve basis.

⁽³⁾ Effectbeoordeling, bijlage A, Methode voor de overdracht van gegevens door de luchtvervoerders.

⁽⁴⁾ Artikel 3 van het voorstel.

⁽¹⁾ Artikel 6 van het voorstel.

Bevoegde autoriteiten

72. Uit artikel 4 van het voorstel blijkt dat iedere autoriteit die verantwoordelijk is voor de voorkoming en bestrijding van terroristische misdrijven en georganiseerde criminaliteit de gegevens kan ontvangen. Hoewel het doel duidelijk is omschreven, ontbreekt de hoedanigheid van de autoriteit. Het voorstel voorziet niet in een beperking van de ontvangers tot wetshandhavingsinstanties.

Zoals hierboven is gezegd met betrekking tot PIU's, is het van doorslaggevend belang dat de desbetreffende gevoelige informatie in een omgeving met een duidelijk rechtskader wordt verwerkt. Dat is bijvoorbeeld veel meer het geval voor wetshandhavingsinstanties dan voor inlichtingendiensten. Gezien de elementen van datamining en proactief onderzoek die het voorstel bevat, kan niet worden uitgesloten dat dergelijke inlichtingendiensten bij de verwerking van de gegevens worden betrokken, zonder uitsluiting van andere soorten autoriteiten.

Conclusie

73. De algemene opmerking van de EDPS is dat de handhaving van een PNR-systeem van de EU zelfs nog moeilijker wordt gemaakt aangezien wetshandhavingsautoriteiten verschillende bevoegdheden hebben naar gelang van het nationale recht van de lidstaten, al dan niet met inbegrip van inlichtingen-, belastingen-, immigratie- of politiediensten. Dit is echter een bijkomende reden om aan te bevelen het voorstel preciezer te maken met betrekking tot de hoedanigheid van de vermelde actoren en de garanties voor toezicht op de uitvoering van hun taken. Er moeten aanvullende bepalingen in het voorstel worden opgenomen, om de bevoegdheden en de wettelijke verplichtingen van intermediairs, PIU's en andere bevoegde autoriteiten duidelijk te specificeren.

V. VOORWAARDEN VOOR DOORGIFFTE AAN DERDE LANDEN

74. Het voorstel voorziet in een aantal waarborgen in verband met de doorgifte van PNR-gegevens aan derde landen⁽¹⁾. Het voorziet met name uitdrukkelijk in de toepassing van het kaderbesluit gegevensbescherming op de doorgifte van gegevens, alsook in een specifieke beperking van het doel, en het bepaalt dat de lidstaat zijn toestemming moet geven in geval van verdere doorgifte. De doorgifte moet ook in overeenstemming zijn met de nationale wetgeving van de betrokken lidstaat, en met alle toepasselijke internationale overeenkomsten.
75. Er blijven echter vele vragen, met name met betrekking tot de aard van de toestemming, de voorwaarden voor toepassing van het kaderbesluit gegevensbescherming en de kwestie van „wederkerigheid” bij de doorgifte van gegevens aan derde landen.

Aard van de toestemming

76. De lidstaat van herkomst moet uitdrukkelijk toestemming geven voor de verdere doorgifte van gegevens door een derde land aan een ander derde land. Het voorstel specificeert niet onder welke voorwaarden en door wie deze toestemming zal worden gegeven en of de nationale gegevensbeschermingsautoriteiten bij het besluit moeten worden betrokken. De EDPS is van oordeel dat de manier waarop toestemming wordt gegeven ten minste in overeenstemming moet zijn met de nationale wetten waarin voorwaarden voor de doorgifte van persoonsgegevens aan derde landen worden gesteld.
77. Bovendien mag toestemming van een lidstaat niet prevaleren boven het beginsel volgens hetwelk het land van ontvangst in een passend niveau van bescherming moet voorzien voor de beoogde verwerking. Deze voorwaarden moeten cumulatief zijn, aangezien zij in het kaderbesluit gegevensbescherming zijn opgenomen (artikel 14). De EDPS stelt derhalve voor het volgende punt c) toe te voegen aan artikel 8, lid 1: „en c) het derde land voor een passend beschermingsniveau voor de beoogde gegevensverwerking zorgt”. De EDPS herinnert er in dit verband aan dat er mechanismen moeten komen die gemeenschappelijke normen en gecoördineerde beslissingen met betrekking tot adequaatheid garanderen⁽²⁾.

Toepassing van het kaderbesluit gegevensbescherming

78. Het voorstel verwijst naar de in het kaderbesluit gegevensbescherming vervatte voorwaarden en waarborgen en specificeert ook uitdrukkelijk een aantal voorwaarden, met name de bovengenoemde toestemming van de betrokken lidstaat, en een beperking van het doel tot de voorkoming en bestrijding van terroristische misdrijven en georganiseerde criminaliteit.
79. Het kaderbesluit gegevensbescherming zelf voorziet in voorwaarden voor de doorgifte van persoonsgegevens aan derde landen, namelijk met betrekking tot de beperking van het doel, de hoedanigheid van de ontvangers, de toestemming van de lidstaten, en het beginsel van adequaatheid. Het voorziet evenwel ook in afwijkingen van deze voorwaarden voor doorgifte: gerechtvaardigde doorslaggevende belangen, met name zwaarwegende openbare belangen, kunnen een voldoende basis voor doorgifte zijn, zelfs indien de hierboven genoemde voorwaarden niet zijn vervuld.
80. Zoals reeds is vermeld in deel III van dit advies, is de EDPS van oordeel dat in de tekst van het voorstel duidelijk moet worden opgenomen dat de meer precieze waarborgen van het voorstel prevaleren boven de algemene voorwaarden — en uitzonderingen — van het kaderbesluit gegevensbescherming, waar dat van toepassing is.

⁽¹⁾ Artikel 8 van het voorstel.

⁽²⁾ Advies van de EDPS van 26 juni 2007 over het voorstel voor een kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politieke en justitiële samenwerking in strafzaken, punten 27 tot en met 30 (PB C 139 van 23.6.2007, blz. 1).

Wederkerigheid*Landen die een bilaterale overeenkomst met de EU hebben*

81. Het voorstel behandelt de kwestie van mogelijke „vergelingsverzoeken” van landen die de EU om PNR-gegevens zouden kunnen verzoeken voor vluchten van de EU naar hun grondgebied. Wanneer de EU om gegevens uit de databanken van luchtvaartmaatschappijen van deze derde landen verzoekt, omdat zij een vlucht naar of vanuit de EU verzorgen, zouden die derde landen hetzelfde kunnen vragen van in de EU gevestigde luchtvaartmaatschappijen, met inbegrip van gegevens van EU-burgers. Hoewel de Commissie dit „vrij onwaarschijnlijk” acht, laat zij het toe. Het voorstel verwijst in dit verband naar het feit dat in de Overeenkomsten met de Verenigde Staten en Canada in een dergelijke „automatisch afdwingbare” wederkerige behandeling is voorzien ⁽¹⁾. De EDPS heeft vragen bij de betekenis van deze automatische wederkerigheid en de toepassing van voorwaarden op dergelijke doorgiften, met name rekening houdend met het bestaan van een passend niveau van bescherming van het betrokken land.
82. Er moet een onderscheid worden gemaakt tussen derde landen die reeds een overeenkomst met de EU hebben gesloten en landen die dat niet hebben gedaan.

Landen die geen overeenkomst met de EU hebben

83. De EDPS neemt er nota van dat wederkerigheid kan leiden tot het doorgeven van persoonsgegevens aan landen die geen garanties kunnen bieden inzake democratische normen en een passend niveau van gegevensbescherming.
84. De effectbeoordeling geeft verdere elementen met betrekking tot de voorwaarden voor doorgifte van gegevens aan derde landen: het voordeel van het PNR-systeem van de EU, waarbij gegevens door PIU's worden gefilterd, wordt benadrukt. Alleen geselecteerde gegevens van verdachte personen (en geen bulkdata) zouden worden doorgegeven aan de bevoegde autoriteiten van de lidstaten en waarschijnlijk ook aan derde landen ⁽²⁾. De EDPS beveelt aan dit punt in de tekst van het voorstel te verduidelijken. Een eenvoudige verklaring in de effectbeoordeling biedt niet de nodige bescherming.
85. Hoewel de selectie van gegevens het effect op de privacy van passagiers mede zou beperken, zij eraan herinnerd dat de beginselen inzake gegevensbescherming veel meer behelzen dan een beperking van het aantal gegevens — namelijk ook noodzakelijkheid, transparantie en de uitoefening van de rechten van de betrokkenen — en dat met alle beginselen rekening moet worden gehouden om te bepalen of een derde land een passend niveau van bescherming biedt.

86. De effectbeoordeling geeft aan dat de EU in dit geval in die bilaterale overeenkomsten met derde landen op bepaalde normen kan aandringen en voor samenhang kan zorgen. Het wordt ook mogelijk derde landen waarmee de EU een overeenkomst heeft, om een wederkerige behandeling te verzoeken, hetgeen nu niet kan ⁽³⁾.

87. Dit doet de vraag rijzen welk effect het voorstel heeft op de bestaande overeenkomsten met Canada en de Verenigde Staten. De voorwaarden voor toegang tot gegevens zijn in die overeenkomsten inderdaad ruimer, omdat de gegevens niet aan een soortgelijke selectie worden onderworpen voordat zij aan die derde landen worden doorgegeven.

88. In de effectbeoordeling wordt gesteld dat in gevallen waarin de EU met een derde land een internationale overeenkomst heeft betreffende de uitwisseling/overdracht van PNR-gegevens aan dat derde land, terdege rekening moet worden gehouden met die overeenkomst. De luchtvervoerders moeten de PNR-gegevens naar de passagiersinformatie-eenheden zenden conform de normale praktijk uit hoofde van de huidige maatregel. De PIU die deze gegevens ontvangt, geeft ze door aan de bevoegde autoriteit van het derde land waarmee een dergelijke overeenkomst bestaat ⁽⁴⁾.

89. Terwijl het voorstel enerzijds ten doel lijkt te hebben *alleen geselecteerde* gegevens door te geven aan bevoegde autoriteiten binnen of buiten de EU, herinneren de effectbeoordeling, de preambule (overweging 21) en artikel 11 zelf er anderzijds aan dat terdege rekening moet worden gehouden met de bestaande overeenkomsten. Dit kan tot de conclusie leiden dat filteren alleen een geldige maatregel kan zijn voor toekomstige overeenkomsten. In dit opzicht zou erin kunnen worden voorzien dat toegang tot de gegevens als „bulk” nog steeds de regel is voor de toegang door, bijvoorbeeld, de autoriteiten van de Verenigde Staten tot PNR-gegevens, overeenkomstig de bepalingen van de Overeenkomst tussen de EU en de Verenigde Staten, maar dat tegelijkertijd en per geval een doorgifte van gegevens aan de Verenigde Staten zou kunnen plaatsvinden die betrekking heeft op door de PIU's vastgestelde specifieke gegevens, met inbegrip van, zij het niet beperkt tot, gegevens betreffende vluchten naar de Verenigde Staten.

90. De EDPS betreurt het gebrek aan duidelijkheid op dit beslissende punt van het voorstel. Hij acht het uiterst belangrijk dat de voorwaarden voor doorgifte van PNR-gegevens aan derde landen coherent zijn en een geharmoniseerd beschermingsniveau genieten. Daarnaast moeten ter wille van de rechtszekerheid verduidelijkingen met betrekking tot de garanties voor de doorgifte van gegevens in het voorstel zelf worden opgenomen en niet alleen in de effectbeoordeling, zoals nu het geval is.

⁽¹⁾ Toelichting bij het voorstel, punt 2.

⁽²⁾ Effectbeoordeling, punt 5.2, Bescherming van de privacy.

⁽³⁾ Effectbeoordeling, punt 5.2, Betrekkingen met derde landen.

⁽⁴⁾ Effectbeoordeling, bijlage A, Instanties die de gegevens van de passagiersinformatie-eenheden ontvangen.

VI. ANDERE BELANGRIJKE PUNTEN

Geautomatiseerde verwerking

91. De EDPS neemt er nota van dat het voorstel uitdrukkelijk uitsluit dat door de passagiersinformatie-eenheden en de bevoegde autoriteiten van de lidstaten handhavingsmaatregelen worden genomen die uitsluitend op geautomatiseerde verwerking van PNR-gegevens of op ras of etnische afstamming, godsdienstige, levensbeschouwelijke of politieke overtuiging of seksuele geaardheid van een persoon zijn gebaseerd ⁽¹⁾.
92. Deze verduidelijking is welkom, aangezien ze het risico van willekeurige maatregelen tegen personen beperkt. De EDPS neemt er evenwel nota van dat het toepassingsgebied wordt beperkt tot *handhavingsmaatregelen* van PIU's of bevoegde autoriteiten. Deze formulering sluit de geautomatiseerde filtering van personen volgens standaardprofielen niet uit, en verhindert evenmin de geautomatiseerde opstelling van lijsten van verdachte personen en het nemen van maatregelen zoals uitgebreid toezicht, zolang deze maatregelen niet als handhavingsmaatregelen worden beschouwd.
93. De EDPS vindt het begrip *handhavingsmaatregelen* te vaag, en is van oordeel dat in principe *geen enkel besluit* met betrekking tot personen zou mogen worden genomen dat *uitsluitend* op de geautomatiseerde verwerking van hun gegevens gebaseerd is ⁽²⁾. De EDPS beveelt aan het voorstel dienovereenkomstig te wijzigen.

Aard van de gegevens

94. Artikel 5, lid 2, van het voorstel bevat een belangrijke precisering, aangezien duidelijk wordt gemaakt dat de luchtvaartmaatschappijen niet worden verplicht om, naast de gegevens die voor het oorspronkelijke commerciële doel worden verzameld, nog andere gegevens te verzamelen of te bewaren.
95. Verscheidene aspecten van de verwerking van die gegevens moeten nog verder worden toegelicht:
- de in bijlage 1 van het voorstel vermelde lijst van beschikbaar te stellen gegevens is zeer uitgebreid en is vergelijkbaar met de lijst van aan de VS-autoriteiten beschikbaar te stellen gegevens die is opgenomen in de Overeenkomst tussen de EU en de Verenigde Staten. De aard van een aantal van de vereiste gegevens is reeds verscheidene malen in twijfel getrokken door de gegevensbeschermingsautoriteiten, met name door de Groep van artikel 29 ⁽³⁾;

⁽¹⁾ Overweging 20 en artikel 3, leden 3 en 5, van het voorstel.

⁽²⁾ Zie in dit verband artikel 15, lid 1, van Richtlijn 95/46/EG. De Richtlijn verbiedt zulke geautomatiseerde besluiten in gevallen waarin personen door het besluit zouden worden getroffen. Wat de context van het voorstel betreft, is het waarschijnlijk dat besluiten in een wetshandhavingskader hoe dan ook zeer ingrijpend kunnen zijn voor de betrokkenen. De betrokkenen kunnen ook worden benadeeld door dat zij aan secundaire controles worden onderworpen, vooral indien dit herhaaldelijk gebeurt.

⁽³⁾ Zie met name Advies nr. 5/2007 van 17 augustus 2007 betreffende de in juli 2007 gesloten vervolgovereenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en overdracht van persoonsgegevens van passagiers (PNR-gegevens) door luchtvaartmaatschappijen aan het *Department of Homeland Security* (ministerie van binnenlandse veiligheid) van de Verenigde Staten van Amerika, WP 138.

- uit de formulering van de effectbeoordeling ⁽⁴⁾ en artikel 6, lid 3, van het voorstel blijkt dat de luchtvaartmaatschappijen de gegevens ook als „bulk” aan intermediairs zouden kunnen overdragen. In een eerste stadium zouden aan een derde partij overgedragen gegevens zelfs niet worden beperkt overeenkomstig de in bijlage 1 van het voorstel opgenomen PNR-gegevens;
- wat de verwerking van gevoelige gegevens betreft, zelfs indien deze gegevens in het stadium van de intermediairs kunnen worden uitgefilterd, blijft de vraag of de doorgifte van open velden door luchtvaartmaatschappijen strikt noodzakelijk is.

De EDPS steunt de punten die in dit verband in het advies van de Groep van artikel 29 zijn gemaakt.

Methode voor de doorgifte van PNR-gegevens

96. Buiten de EU gevestigde luchtvaartmaatschappijen wordt verzocht gegevens zelf door te geven aan PIU's of intermediairs („push-methode”), voor zover zij over de nodige technische architectuur beschikken. Indien dat niet het geval is, zullen zij de overname van gegevens via de „pull-methode” moeten toestaan.
97. Het toestaan van verschillende methoden voor de verstrekking van gegevens naar gelang van de betrokken luchtvaartmaatschappijen zal des te meer moeilijkheden opleveren met betrekking tot de controle op de overeenstemming van de doorgifte van PNR-gegevens met de gegevensbeschermingsregels. Dit dreigt ook de concurrentie tussen luchtvaartmaatschappijen van binnen en buiten de EU te verstoren.
98. De EDPS herinnert eraan dat de push-methode, waarbij de luchtvaartmaatschappijen toezicht kunnen blijven houden op de kwaliteit van de doorgegeven gegevens en de omstandigheden van de doorgifte, de enige toelaatbare methode is wat betreft de evenredigheid van de verwerking. Bovendien moet het een daadwerkelijke „push” zijn, dat wil zeggen dat de gegevens niet als „bulk” aan een intermediair mogen worden gezonden, maar dat ze vanaf de eerste fase van de verwerking moeten worden gefilterd. Het is niet toelaatbaar dat niet-noodzakelijke gegevens — en gegevens die niet in bijlage 1 van het voorstel zijn opgenomen — aan een derde partij worden toegezonden, ook al moeten deze onmiddellijk door deze derde partij worden gewist.

Gegevensbewaring

99. Artikel 9 van het voorstel voorziet in een bewaringstermijn van 5 jaar voor PNR-gegevens, met een bijkomende termijn van 8 jaar waarin de gegevens moeten worden bijgehouden in een „slappende” databank die onder beperkte voorwaarden toegankelijk zal zijn.

⁽⁴⁾ Effectbeoordeling, bijlage A, Methode voor de overdracht van gegevens door de luchtvervoerders.

100. De EDPS heeft vragen bij het verschil tussen de twee soorten databanken: het is twijfelachtig of de slapende databank een echt archief is, met verschillende methoden voor de opslag en opvraging van gegevens. De meeste van de voorwaarden voor toegang tot de slapende databank bestaan immers uit veiligheidsvoorschriften die ook voor de „databank voor bewaring gedurende vijf jaar” zouden kunnen gelden.

101. De totale opslagduur — 13 jaar — is in ieder geval buitensporig lang. Deze wordt in de effectbeoordeling gerechtvaardigd door de noodzaak om risico-indicatoren te ontwikkelen en reis- en gedragspatronen af te leiden ⁽¹⁾, waarvan de efficiëntie nader moet worden aangetoond. Hoewel het duidelijk is dat, bij een lopend onderzoek gegevens in een specifiek geval zolang als nodig kunnen worden bewaard, valt het niet te rechtvaardigen dat de gegevens van alle passagiers 13 jaar lang worden bewaard, terwijl er geen sprake is van enige vorm van verdenking.

102. De EDPS neemt er verder nota van dat de lidstaten in hun antwoorden op de vragenlijst van de Commissie niet achter deze bewaringstermijn staan; volgens deze antwoorden zou de gemiddelde duur van de bewaringstermijn 3,5 jaar zijn ⁽²⁾.

103. Bovendien is de termijn van 13 jaar vergelijkbaar met de bewaringstermijn van 15 jaar in de meest recente overeenkomst met de Verenigde Staten. De EDPS heeft altijd aangenomen dat deze lange bewaringstermijn alleen was overeengekomen omdat de VS-regering sterke druk uitoefende om een veel langere termijn dan 3,5 jaar te bekomen, en niet omdat dit ooit door de Raad of de Commissie werd verdedigd. Er is geen reden om een dergelijk compromis — dat alleen is gerechtvaardigd als noodzakelijk resultaat van onderhandelingen — binnen de EU zelf in een rechtsinstrument om te zetten.

Rol van het comité van de lidstaten

104. Het comité van de lidstaten dat op grond van artikel 14 van het voorstel wordt opgericht, zal bevoegd zijn voor beveiligingskwesties met inbegrip van protocollen en versleuteling van PNR-gegevens, maar ook voor advies inzake gemeenschappelijke algemene criteria en werkmethoden voor de risicobeoordeling.

105. Behalve deze indicaties bevat het voorstel geen elementen of criteria met betrekking tot de concrete voorwaarden en het concrete kader van het risicobeoordelingsproces. De effectbeoordeling vermeldt dat de criteria uiteindelijk zullen afhangen van de inlichtingen die in het bezit van iedere lidstaat zijn en die in voortdurende ontwikkeling

zijn. De risicobeoordeling moet worden verricht zonder dat er eenvormige normen voor de identificatie van verdachten zijn. De mate waarin het comité van de lidstaten in dit opzicht een rol zal kunnen spelen, lijkt dus twijfelachtig.

Beveiliging

106. Het voorstel bevat een reeks beveiligingsmaatregelen ⁽³⁾ die door PIU's, intermediairs en andere bevoegde autoriteiten moeten worden genomen om de gegevens te beschermen. Gezien het belang van de databank en de gevoelige aard van de verwerking, is de EDPS van oordeel dat, naast de beoogde maatregelen, de entiteit die de gegevens verwerkt ook moet worden verplicht om officieel kennis te geven van iedere inbreuk op de beveiliging.

107. De EDPS is op de hoogte van het project om op Europees niveau een dergelijke kennisgevingsprocedure in te stellen in de elektronischecomunicatiesector. Hij adviseert deze waarborg op te nemen in het onderhavige voorstel, en verwijst in dit verband naar het systeem voor inbreuken op de beveiliging dat in de Verenigde Staten is ingevoerd met betrekking tot overheidsdiensten ⁽⁴⁾. Er kunnen zich namelijk beveiligingsincidenten voordoen op alle activiteitsterreinen, zowel in de particuliere als in de openbare sector, zoals het recente verlies van een volledige databank met gegevens van burgers door de Britse administratie heeft aangetoond ⁽⁵⁾. Grootschalige databanken zoals degene die in het voorstel wordt beoogd, zouden bij voorrang met een dergelijk waarschuwingssysteem moeten worden uitgerust.

Evaluatie- en vervalbepaling

108. De EDPS neemt er nota van dat er binnen drie jaar na de inwerkingtreding van het kaderbesluit een evaluatie moet plaatsvinden op basis van een verslag van de Commissie. Hij erkent dat deze evaluatie, die gebaseerd zal zijn op door de lidstaten verstrekte informatie, specifiek betrekking zal hebben op gegevensbeschermingswaarborgen, en de toepassing van de „push-methode”, de gegevensbewaring en de kwaliteit van de risicobeoordeling zal omvatten. Volledigheidshalve moet deze evaluatie de resultaten bevatten van een analyse van de statistische gegevens die op basis van de verwerking van PNR-informatie zijn geproduceerd. Deze statistieken moeten, naast de in artikel 18 van het voorstel vermelde elementen, nadere statistische gegevens betreffende de identificatie van personen met een hoog risico bevatten, zoals de criteria voor die identificatie en de concrete resultaten van wets-handhavingsacties ten gevolge van de identificatie.

⁽³⁾ Artikel 12 van het voorstel.

⁽⁴⁾ Zie met name het werk van de Amerikaanse „Identity Theft Task Force”:

<http://www.idtheft.gov/>

⁽⁵⁾ Zie de link naar de website van de Britse douane:

<http://www.hmrc.gov.uk/childbenefit/update-faqs.htm>

Zie ook:

http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

⁽¹⁾ Effectbeoordeling, bijlage A, Termijn voor de bewaring van gegevens.

⁽²⁾ Effectbeoordeling, bijlage B.

109. De EDPS heeft in dit advies reeds de klemtoon gelegd op het ontbreken van concrete elementen om de noodzakelijkheid van het voorgestelde systeem vast te stellen. Hij is echter van mening dat, wanneer het kaderbesluit in werking treedt, het ten minste moet worden aangevuld met een vervalbepaling. Aan het eind van de periode van drie jaar moet het kaderbesluit worden ingetrokken indien er geen elementen zijn die pleiten voor verlenging.

Effect op andere rechtsinstrumenten

110. In de slotbepalingen van het voorstel wordt een voorwaarde gesteld voor de verdere toepassing van bestaande bilaterale of multilaterale overeenkomsten of regelingen. Die instrumenten kunnen slechts worden toegepast voor zover zij verenigbaar zijn met de doelstellingen van het voorgestelde kaderbesluit.

111. De EDPS heeft twijfels bij het toepassingsgebied van deze bepaling. Zoals reeds in deel V onder „Wederkerigheid” is vermeld, is het niet duidelijk wat het effect van deze bepaling zal zijn op de inhoud van overeenkomsten met derde landen, zoals de overeenkomst met de Verenigde Staten. Vanuit een ander perspectief is het evenmin duidelijk of de bepaling een effect kan hebben op de voorwaarden voor toepassing van instrumenten met een ruimer toepassingsgebied, zoals Verdrag nr. 108 van de Raad van Europa. Hoewel dit onwaarschijnlijk kan lijken gezien het verschil in institutionele context en betrokken actoren, moet ieder risico op verkeerde interpretatie worden vermeden en moet het voorstel duidelijk maken dat het geen effect heeft op instrumenten met een ruimer toepassingsgebied, met name degenen die betrekking hebben op de bescherming van de grondrechten.

VII. CONCLUSIE

112. De EDPS benadrukt de ingrijpende gevolgen van het huidige voorstel qua de gegevensbescherming. Hij heeft zijn analyse toegespitst op vier fundamentele kwesties die in het voorstel aan de orde komen, en beklemtoont dat de aangehaalde kwesties integraal moeten worden aangepakt. In de huidige omstandigheden is het voorstel niet in overeenstemming met de grondrechten, met name met artikel 8 van het Handvest van de grondrechten van de Unie, en zou het niet mogen worden aangenomen.

113. Indien gehoor wordt gegeven aan de bovenstaande opmerkingen, met name betreffende de rechtmatigheidstoets, dan moet de wetgever rekening houden met een aantal formuleringsvoorstellen die in dit advies zijn gedaan. Met name wordt verwezen naar de punten 67, 73, 77, 80, 90, 93, 106, 109 en 111 van het advies.

Rechtmatigheid van de voorgestelde maatregelen

114. Hoewel het algemene doel van bestrijding van terrorisme en georganiseerde criminaliteit op zich duidelijk en rechtmatig is, is de essentie van de te verrichten verwerking niet voldoende omschreven en verantwoord.

115. De EDPS is van oordeel dat de technieken om het risico dat bepaalde personen vormen te beoordelen door middel van datamininginstrumenten en gedragspatronen, verder moeten worden geëvalueerd, en dat hun nut voor terrorismebestrijding duidelijk moet worden vastgesteld alvorens zij op zo'n grote schaal worden gebruikt.

116. Voortbouwen op verschillende databanken zonder algemeen zicht op de concrete resultaten en tekortkomingen:

— is in strijd met een rationeel wetgevingsbeleid waarin nieuwe instrumenten niet mogen worden aangenomen voordat de bestaande instrumenten volledig uitgevoerd zijn en onvoldoende gebleken zijn;

— kan er toe leiden dat wij evolueren naar een totaal gecontroleerde samenleving.

117. Terrorismebestrijding kan zeker een legitieme grond zijn om uitzonderingen op de fundamentele rechten op privacy en gegevensbescherming te hanteren. Om geldig te zijn echter moet de noodzakelijkheid van de inbreuk met duidelijke en onweerlegbare elementen worden ondersteund, en moet de evenredigheid van de verwerking worden aangetoond. Dit geldt des te meer bij een grote inbreuk op de persoonlijke levenssfeer, zoals dit voorstel beoogt.

118. Deze verantwoordingselementen ontbreken in het voorstel, dat de noodzakelijkheids- en de evenredigheidstoets niet kan doorstaan.

119. De EDPS benadrukt het essentiële karakter van de bovengenoemde noodzakelijkheids- en evenredigheidstoets. Deze vormt een *conditio sine qua non* voor de inwerkingtreding van het voorstel.

Toepasselijk rechtskader

120. De EDPS neemt nota van een ernstig gebrek aan rechtszekerheid met betrekking tot de regeling die van toepassing is op de verschillende bij het project betrokken actoren, met name luchtvaartmaatschappijen en andere actoren uit de eerste pijler, of dit nu de regels van het voorstel, de regels van het kaderbesluit gegevensbescherming of de nationale wetgeving ter uitvoering van Richtlijn 95/46/EG zijn. De wetgever moet duidelijk maken in welke fasen van de verwerking deze verschillende regels zullen gelden.

121. De huidige tendens om systematisch samenwerking voor wetshandavingsdoeleinden op te leggen aan particuliere actoren doet de vraag rijzen welk gegevensbeschermingskader (eerste of derde pijler) van toepassing is op de voorwaarden van deze samenwerking; het is niet duidelijk of de regels op de hoedanigheid van de verantwoordelijke voor de verwerking (particuliere sector) of op het beoogde doel (wetshandaving) moeten worden gebaseerd.

122. De EDPS heeft reeds de klemtoon gelegd op het risico van een juridisch vacuüm tussen activiteiten in de eerste en de derde pijler ⁽¹⁾. Het is inderdaad verre van duidelijk of activiteiten van particuliere bedrijven die in zekere zin verband houden met de wetshandhaving op strafrechtelijk gebied, tot het werkkterrein van de wetgever van de Europese Unie uit hoofde van de artikelen 30, 31 en 34 EU-Verdrag behoren.
123. Vermeden moet worden dat verwerking door dienst aanbieders voor verschillende doeleinden aan verschillende kaders voor gegevensbescherming zou worden onderworpen, met name gezien de moeilijkheden die dit zou veroorzaken op het gebied van de uitoefening van de rechten van de betrokkenen.

Hoedanigheid van de ontvangers

124. Het voorstel dient in een specificatie te voorzien met betrekking tot de hoedanigheid van de ontvangers van door luchtvaartmaatschappijen verzamelde persoonsgegevens, hetzij intermediairs, passagiersinformatie-eenheden of bevoegde autoriteiten.
125. De hoedanigheid van de ontvangers, die in een aantal gevallen actoren uit de particuliere sector kunnen zijn, houdt rechtstreeks verband met het soort garanties inzake gegevensbescherming die voor die ontvanger gelden. Het is van essentieel belang dat de toepasselijke regeling duidelijk is voor alle betrokken actoren, waaronder de wetgever, de gegevensbeschermingsautoriteiten, alsook de verantwoordelijken voor de verwerking en de betrokkenen.

Doorgifte van gegevens aan derde landen

126. De EDPS benadrukt dat ervoor moet worden gezorgd dat in het land van ontvangst in een passend niveau van bescherming wordt voorzien. Hij heeft ook vragen bij de betekenis van het in het voorstel vermelde „wederkerigheidsbeginsel” en de toepassing ervan op landen die reeds gebonden zijn door een overeenkomst met de EU, zoals Canada of de Verenigde Staten. Hij acht het uiterst belangrijk dat de voorwaarden voor doorgifte van PNR-gegevens aan derde landen coherent zijn en een geharmoniseerd beschermingsniveau genieten.

Andere belangrijke punten

127. De EDPS vestigt ook de aandacht van de wetgever op specifieke aspecten van het voorstel die moeten worden verduidelijkt of die beter rekening moeten houden met het gegevensbeschermingsbeginsel. Dit is met name het geval met betrekking tot de volgende aspecten:
- de voorwaarden waaronder geautomatiseerde besluiten kunnen worden genomen, moeten worden beperkt;
 - de verwerkte gegevens moeten van mindere „kwaliteit” zijn;
 - de methode voor doorgifte van gegevens mag alleen op „push” berusten;
 - de termijn voor de bewaring van gegevens wordt als buitensporig lang en niet gerechtvaardigd beschouwd;
 - de rol van het comité van de lidstaten kan preciezer worden omschreven met betrekking tot zijn adviesverlening inzake „risicobeoordeling”;
 - de beveiligingsmaatregelen moeten een procedure voor „kennisgeving van inbreuk op de beveiliging” omvatten;
 - met het oog op de evaluatie van het besluit moet in een vervalbepaling worden voorzien;
 - het voorstel moet duidelijk maken dat het geen effect heeft op instrumenten met een ruimer toepassingsgebied die met name betrekking hebben op de bescherming van de grondrechten.

Slotopmerkingen

128. De EDPS neemt er nota van dat het onderhavige voorstel op een ogenblik komt waarop de institutionele context van de Europese Unie op het punt staat fundamenteel te wijzigen. De gevolgen van het Verdrag van Lissabon op het gebied van besluitvorming zullen fundamenteel zijn, vooral wat de rol van het Parlement betreft.
129. Het nooit eerder geziene effect van het voorstel met betrekking tot de grondrechten in aanmerking nemend, adviseert de EDPS dit voorstel niet aan te nemen in het kader van het huidige Verdrag, maar ervoor te zorgen dat het de medebeslissingsprocedure van het nieuwe Verdrag volgt. Dat zou de rechtsgrondslagen versterken waarop de in het voorstel beoogde beslissende maatregelen zullen worden genomen.

⁽¹⁾ Zie het Advies van de Europese Toezichthouder voor gegevensbescherming inzake de mededeling van de Commissie aan het Europees Parlement en de Raad over de follow-up van het werkprogramma voor een betere toepassing van de richtlijn gegevensbescherming (PB C 255 van 27.10.2007, blz. 1). Zie ook het Jaarverslag 2006, blz. 47.