I

(Resoluties, aanbevelingen en adviezen)

ADVIEZEN

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING

Advies van de Europese Toezichthouder voor gegevensbescherming over het eindverslag van de EU-VS-Contactgroep op hoog niveau inzake informatie-uitwisseling en privacy en bescherming van persoonsgegevens

(2009/C 128/01)

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,

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, en met name op artikel 41,

BRENGT HET VOLGENDE ADVIES UIT:

I. INLEIDING — CONTEXT VAN HET ADVIES

1. Met het oog op de EU-top van 12 juni 2008 deelde het voorzitterschap van de Raad van de Europese Unie op 28 mei 2008 aan het Coreper mee dat de EU-VS-Contactgroep op hoog niveau (hierna de HLCG) inzake informatie-uitwisseling en privacy en de bescherming van persoonsgegevens zijn verslag had voltooid. Dit verslag werd op 26 juni 2008 ([1]) gepubliceerd.

2. Het verslag heeft als doel gezamenlijke beginselen voor privacy en gegevensbescherming te bepalen, als eerste stap naar informatie-uitwisseling met de Verenigde Staten in de strijd tegen terrorisme en ernstige grensoverschrijdende misdaad.

3. In zijn mededeling laat het voorzitterschap van de Raad weten dat het zich aanbevolen houdt voor ideeën voor de follow-up van het verslag, met name voor reacties op de hierin aanbevolen mogelijkheden. De EDPS brengt daarom het volgende advies uit, op basis van de gemelde stand van zaken en onverminderd de standpunten die de EDPS gaandeweg zou kunnen innemen.

4. De EDPS merkt op dat de werkzaamheden van de HLCG hebben plaatsgevonden in een context waarin, vooral sinds 11 september 2001, de gegevensuitwisseling tussen de VS en de EU verder is ontwikkeld middels internationale overeenkomsten of andere vormen van regelgeving. Daartoe behoren onder meer de overeenkomsten van Europol en Eurojust met de Verenigde Staten, alsook de PNR-overeenkomsten en de zaak SWIFT, die heeft geleid tot een briefwisseling tussen EU- en VS-ambtenaren om minimumwaarborgen voor gegevensbescherming vast te stellen ([2]).

([1]) Document van de Raad nr. 9831/08, beschikbaar op http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

([2]) — Overeenkomst tussen de Verenigde Staten van Amerika en de Europese Politiedienst van 6 december 2001, en aanvullende overeenkomst tussen Europol en de VS inzake de uitwisseling van persoonsgegevens en daarmee verbonden informatie, gepubliceerd op de website van Europol;
— Overeenkomst tussen de Verenigde Staten van Amerika en Eurojust inzake justitiële samenwerking, 6 november 2006, gepubliceerd op de website van Eurojust;
— Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en de overdracht van persoonsgegevens van passagiers (PNR-gegevens) door luchtvaartmaatschappijen aan het ministerie van Binnenlandse van 23 juli 2007 veiligheid van de Verenigde Staten van Amerikavan 26 juli 2007 (PNR-Overeenkomst 2007), PB L 204 van 4.8.2007, blz. 18.
— Briefwisseling tussen de VS- en de EU-autoriteiten inzake het programma voor het opsporen van de financiering van terroristische activiteiten, 28 juni 2007.

5. Voorts worden dergelijke regels voor de uitwisseling van persoonsgegevens ook met andere landen besproken en vastgesteld. Een recent voorbeeld is de Overeenkomst tussen de Europese Unie en Australië inzake de verwerking en overdracht van persoonsgegevens van passagiers (PNR-gegevens) uit de Europese Unie door luchtvaartmaatschappijen aan de Australische douane ([3]).

6. Uit het bovenstaande blijkt dat de vraag van de wetshandhavingsautoriteiten van derde landen naar persoonsgegevens voortdurend toeneemt, en naast traditionele overheidsgegevensbanken ook andere soorten bestanden, met name door de privésector samengestelde gegevensbanken, omvat.

7. Voorts is het van belang dat de overdracht van persoonsgegevens aan derde landen in het kader van politiële en justitiële samenwerking in strafzaken ook wordt geregeld in het gelijknamige kaderbesluit van de Raad ([4]), dat naar verwachting vóór eind 2008 zal worden aangenomen.

8. Verwacht wordt dat deze trans-Atlantische informatie-uitwisseling alleen maar zal toenemen en zich zal uitbreiden tot andere sectoren waar persoonsgegevens worden verwerkt. In een dergelijke context komt een dialoog over „trans-Atlantische wetshandhaving" gelegen, maar hij is ook delicaat. De dialoog komt gelegen, omdat hij een duidelijker kader kan scheppen voor gegevensuitwisseling, nu en in de toekomst. Een dergelijke dialoog is echter ook delicaat, omdat dit kader de legitimatie zou kunnen vormen voor massale gegevensoverdracht op een gebied — wetshandhaving — met een bijzonder grote impact op personen en waarop strenge en betrouwbare waarborgen en garanties des te noodzakelijker zijn ([5]).

9. In het volgende hoofdstuk worden de stand van zaken en de mogelijkheden besproken. Hoofdstuk III is gewijd aan het toepassingsgebied en de vorm van een regeling die informatie-uitwisseling mogelijk maakt. In hoofdstuk IV worden vanuit een algemeen oogpunt de inhoudelijke juridische aspecten van een mogelijke overeenkomst geanalyseerd. Er komen kwesties aan bod zoals de beoordelingscriteria van het beschermingsniveau in de Verenigde Staten, en het gebruik van het regelgevingskader van de EU als een *benchmark* om dit beschermingsniveau te beoordelen. Het hoofdstuk bevat ook een overzicht van de basisvereisten die in een dergelijke overeenkomst moeten worden opgenomen. Tot slot worden in hoofdstuk V de bij het verslag gevoegde privacybeginselen geanalyseerd.

II. **STAND VAN ZAKEN EN MOGELIJKHEDEN.**

10. Hierna volgt de beoordeling van de stand van zaken door de EDPS. Er is vooruitgang geboekt bij het bepalen van gezamenlijke normen voor informatie-uitwisseling en de bescherming van persoonsgegevens.

11. De voorbereidingen voor een overeenkomst tussen de EU en de VS, ongeacht de vorm, zijn echter nog niet afgerond, en extra inspanningen zijn noodzakelijk. In het verslag van de HLCG zelf zijn een aantal niet-afgehandelde kwesties vermeld, waarvan de belangrijkste die van de „beroepsmogelijkheden" is. Er is nog geen overeenstemming over het noodzakelijke toepassingsgebied van de rechtsmiddelen ([6]). Vijf andere openstaande kwesties zijn in hoofdstuk 3 van het verslag vermeld. Uit dit advies zal blijken dat er nog veel hangpunten zijn, bijvoorbeeld inzake het toepassingsgebied en de vorm van een regeling voor informatie-uitwisseling.

12. Aangezien in het verslag de voorkeur uitgaat naar een bindende overeenkomst — de EDPS deelt deze voorkeur — is des te meer voorzichtigheid geboden. Een overeenkomst zal verder zorgvuldig en grondig moeten worden voorbereid.

13. Tot besluit is de EDPS van mening dat een overeenkomst het best zou worden gesloten op grond van het Verdrag van Lissabon, maar dit hangt natuurlijk af van de inwerkingtreding ervan. Met het Verdrag van Lissabon wordt juridische onzekerheid over de scheidingslijn tussen de EU-pijlers namelijk vermeden. Bovendien worden zo de volledige betrokkenheid van het Europees Parlement en de rechterlijke toetsing door het Hof van Justitie verzekerd.

14. Onder de huidige omstandigheden verdient het de voorkeur een routekaart op te stellen voor een eventuele latere overeenkomst. Deze routekaart zou dan de volgende elementen kunnen bevatten:

— richtsnoeren voor verdere werkzaamheden van de HLCG (of een andere groep) en een tijdschema;

— de bespreking en mogelijke vaststelling van fundamentele kwesties, zoals het toepassingsgebied en de vorm van de overeenkomst;

— de verdere ontwikkeling van de gegevensbeschermingsbeginselen, op basis van een gezamenlijke visie op deze fundamentele kwesties;

— het betrekken van stakeholders bij de verschillende fasen van de procedure;

— het aanpakken van de institutionele hindernissen op Europees niveau.

([3]) PB L 213, van 8.8.2008, blz. 49.

([4]) Kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, versie van 24 juni 2008, beschikbaar op http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371

([5]) Wat de noodzaak van een duidelijk juridisch kader betreft, zie hoofdstukken III en IV van dit advies.

([6]) Blz. 5 van het verslag, punt C.

III. **TOEPASSINGSGEBIED EN VORM VAN EEN AKKOORD OVER INFORMATIE-UITWISSELING**

15. Volgens de EDPS is het van cruciaal belang dat het toepassingsgebied en de vorm van een tekst met gegevensbeschermingsbeginselen, als een eerste stap in de verdere ontwikkeling ervan, duidelijk worden bepaald.

16. Wat het toepassingsgebied betreft, moeten belangrijke vragen worden beantwoord:

— wie zijn de betrokken actoren op het gebied van wetshandhaving en daarbuiten;

— wat wordt verstaan onder „met wetshandhaving als doel", en hoe staat dit in verhouding tot de andere doelen, zoals nationale veiligheid en meer in het bijzonder grenscontrole en volksgezondheid;

— hoe passen de voorschriften in het kader van een grote trans-Atlantische ruimte van veiligheid?

17. De vorm van de regeling zou duidelijkheid moeten scheppen op de volgende punten:

— In welke pijler komt, in voorkomend geval, het akkoord tot stand?

— Is het akkoord bindend voor de partijen?

— Heeft het rechtstreekse werking, in die zin dat het persoonlijke rechten en verplichtingen bevat die in rechte kunnen worden afgedwongen?

— Maakt het akkoord zelf de informatie-uitwisseling mogelijk, of bepaalt het minimumnormen daarvoor, die met specifieke overeenkomsten moeten worden aangevuld?

— Hoe verhoudt het akkoord zich tot de bestaande regelingen; is het eraan ondergeschikt, vervangt het ze of vult het ze aan?

III. 1. **Toepassingsgebied**

Betrokken actoren

18. Hoewel de HLCG het toepassingsgebied niet duidelijk aangeeft, kan uit de door hun vermelde beginselen worden afgeleid dat het zowel de overdrachten tussen particuliere en overheidsactoren ([7]) als tussen overheidsinstanties omvat.

([7]) Zie vooral hoofdstuk 3 van het verslag, „Outstanding issues pertinent to transatlantic relations", punt 1: „Consistency in private entities obligations during data transfers".

— Tussen particuliere en overheidsactoren:

19. De EDPS begrijpt de logica van de toepasselijkheid op overdracht tussen particuliere en overheidsactoren. Het akkoord komt tot stand in het kader van de recente Amerikaanse verzoeken om informatie van particuliere actoren. De EDPS merkt op dat, vanuit het oogpunt van wetshandhaving, particuliere actoren zowel op EU-niveau als internationaal een systematische informatiebron worden ([8]). De zaak SWIFT, waarin een privé-onderneming door de wetshandhavingsautoriteiten van een derde land werd verzocht systematisch en op grote schaal gegevens door te geven, was een belangrijk precedent hiervoor ([9]). De verzameling van PNR-gegevens door luchtvaartmaatschappijen volgt dezelfde logica. In zijn advies betreffende een ontwerpkaderbesluit voor een Europees PNR-systeem heeft de EDPS de rechtmatigheid van deze trend ter discussie gesteld ([10]).

20. Er zijn nog twee bezwaren tegen het inlassen van overdracht tussen particuliere en overheidsactoren in het toepassingsgebied.

21. Ten eerste zou dit een ongewenst effect kunnen hebben binnen de EU zelf. De EDPS is zeer bezorgd dat, indien gegevens van privébedrijven (zoals financiële instellingen) in principe naar derde landen kunnen worden overgedragen, dit de druk zou kunnen vergroten om dergelijke gegevens ook binnen de EU voor wetshandhavingsautoriteiten beschikbaar te stellen. Een voorbeeld van zulke ongewenste ontwikkelingen is de PNR-regeling, die bij aanvang het op grote schaal verzamelen van passagiersgegevens door de VS betrof, en daarna ook werd overgezet op de interne Europese context ([11]), zonder dat de noodzakelijkheid en evenredigheid van het systeem duidelijk waren bewezen.

22. Ten tweede heeft de EDPS in zijn advies betreffende het Commissievoorstel voor EU-PNR ook de vraag opgeworpen welk gegevensbeschermingkader (eerste of derde pijler) van toepassing is op de samenwerking tussen de particuliere en overheidsactoren. Is de hoedanigheid van de verantwoordelijke voor de verwerking (particuliere sector)

([8]) Zie in dit verband het advies van de EDPS van 20 december 2007 betreffende het voorstel voor een kaderbesluit van de Raad over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor wetshandhavingsdoeleinden, PB C 110 van 1.5.2008, blz. 1. „Van oudsher is er een duidelijke scheiding tussen wetshandhaving en activiteiten van de particuliere sector, waarbij wetshandhavingstaken door speciaal daarvoor bevoegde autoriteiten, met name de politiediensten, worden vervuld en particuliere actoren per geval wordt verzocht om persoonsgegevens te verstrekken aan deze handhavingsautoriteiten. Er is nu een tendens om systematisch samenwerking voor wetshandhavingsdoeleinden op te leggen aan particuliere actoren".

([9]) Zie advies 10/2006 van de Groep artikel 29 van 22 november 2006 over de verwerking van persoonsgegevens door de *Society for Worldwide Interbank Financial Telecommunication* (SWIFT), WP 128.

([10]) Advies van 20 december 2007, op. cit.

([11]) Zie het in voetnoot 8 vermelde voorstel voor een kaderbesluit van de Raad over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor wetshandhavingsdoeleinden, dat momenteel in de Raad wordt besproken.

dan wel het beoogde doel (wetshandhaving) bepalend? De scheidingslijn tussen de eerste en derde pijler is verre van duidelijk indien particuliere actoren worden verplicht om persoonsgegevens met het oog op wetshandhaving te verwerken. In deze context is het opvallend dat advocaat-generaal Bot in zijn recente conclusie in de zaak rond het bewaren van gegevens ([12]) een scheidingslijn voorstelt voor dergelijke situaties, maar daarbij tegelijk verklaart: „Deze scheidingslijn is zeker niet vrij van elke kritiek en kan in bepaalde opzichten kunstmatig lijken." De EDPS merkt ook op dat het PNR-arrest van het Hof ([13]) geen uitsluitsel geeft over het toepasselijke juridische kader. Zo betekent het feit dat bepaalde activiteiten niet onder Richtlijn 95/46/EG vallen niet automatisch dat zij in de derde pijler kunnen worden geregeld. De wet kan bijgevolg nog mazen blijven vertonen en in elk geval rechtsonzekerheid ten aanzien van de juridische waarborgen voor de betrokkenen opleveren.

23. De EDPS vindt daarom dat een akkoord met algemene gegevensbeschermingsbeginselen op zich geen legitimatie mag zijn voor trans-Atlantische overdracht van persoonsgegevens tussen particuliere en overheidsactoren. Een dergelijke overdracht kan alleen worden toegestaan mits:

— bewezen wordt dat zij absoluut noodzakelijk is voor een specifiek, per geval bepaald doel;

— de overdracht zelf gebeurt onder strenge gegevensbeschermingsvoorwaarden (zoals beschreven in dit advies).

Voorts merkt de EDPS de onzekerheid op over het toepasselijke gegevensbeschermingskader, en hij pleit er dan ook voor om onder geen beding de overdracht van persoonsgegevens tussen particuliere en overheidsactoren in te voegen in het EU-recht onder de huidige vorm.

— Tussen overheidsinstanties:

24. Het exacte toepassingsgebied van de informatie-uitwisseling is onduidelijk. Als eerste stap moet worden verduidelijkt welk toepassingsgebied wordt beoogd:

— Wat gegevensbanken in de EU betreft — gecentraliseerde gegevensbanken die (deels) door de EU worden beheerd, zoals de Europol- en Eurojustgegevensbanken, of gedecentraliseerde gegevensbanken die door de lidstaten worden beheerd, of beide?

— Ook gekoppelde netwerken, dat wil zeggen, gelden de voorziene waarborgen ook voor gegevens die tussen lidstaten of agentschappen in de EU en de VS worden uitgewisseld?

— Alleen de uitwisseling tussen wetshandhavingsdatabanken (politie, justitie, mogelijks douane), of ook tussen andere, bijvoorbeeld fiscale databanken?

— Ook gegevensbanken van nationale veiligheidsdiensten? Zouden deze diensten toegang krijgen tot wetshandhavingsdatabanken van de andere partij (EU tot VS en omgekeerd)?

— Informatieoverdracht per geval, of permanente toegang tot bestaande gegevensbanken? De tweede mogelijkheid zou zeker vragen in verband met de evenredigheid oproepen, zoals ook besproken in hoofdstuk V, punt 3.

Wetshandhaving als doel

25. Ook het doel van de overeenkomst is ongewis. In de inleiding en in het eerste beginsel bij het verslag is duidelijk sprake van wetshandhaving. Daar wordt in hoofdstuk IV van dit advies dieper op ingegaan. De EDPS merkt nu al op dat blijkens het verslag de uitwisseling van gegevens de derde pijler zou betreffen. De vraag is echter of dit niet een eerste stap is naar een bredere informatie-uitwisseling. Tot de doeleinden van „openbare veiligheid" die in het verslag worden aangehaald, behoort ook de strijd tegen terrorisme, georganiseerde misdaad en andere misdaden. Wordt hiermee echter ook bedoeld de uitwisseling van gegevens voor een ander algemeen belang, bijvoorbeeld in verband met risico's voor de volksgezondheid?

26. De EDPS pleit ervoor dat alleen de verwerking van nauwkeurig bepaalde gegevens onder de overeenkomst wordt gebracht, en dat de beleidskeuzes die daaraan ten grondslag liggen, worden gerechtvaardigd.

([12]) Conclusie van advocaat-generaal Bot van 14 oktober 2008, Ierland tegen Europees Parlement en Raad, (Zaak C-301/06), punt 108.

([13]) Arrest van het Hof van 30 mei 2006 in de gevoegde zaken C-317/04, Europees Parlement tegen Raad van de Europese Unie, en C-318/04, Europees Parlement tegen Commissie van de Europese Gemeenschappen, Jurispr. 2006, blz. I-4721.

Een globale trans-Atlantische ruimte van veiligheid

27. Het brede toepassingsgebied van dit verslag moet worden gezien in het licht van de algehele trans-Atlantische ruimte van veiligheid die door de zogenaamde Toekomstgroep ([14]) wordt besproken. Het in juni 2008 gepubliceerde verslag van deze groep belicht de externe dimensie van het binnenlandsezakenbeleid. De groep vindt dat „*tegen 2014(...) de Europese Unie zich ook (moet) uitspreken over de politieke doelstelling om met de Verenigde Staten een Europees-Atlantische samenwerkingsruimte van vrijheid, veiligheid en recht tot stand te brengen*". Deze samenwerking zou verder gaan dan veiligheid *sensu stricto* en zou ten minste de thema's uit Titel IV van het EG-Verdrag omvatten, zoals immigratie, visa, asiel en justitiële samenwerking in burgerlijke zaken. Daarbij moet de vraag worden gesteld in hoeverre een overeenkomst over grondbeginselen voor gegevensbescherming, bijvoorbeeld die uit het verslag van de HLCG, de basis kan en moet vormen voor informatie-uitwisseling op zo'n uitgestrekt terrein.

28. Normaal gezien zal de pijlerstructuur tegen 2014 niet langer bestaan en zal er binnen de EU één rechtsgrondslag voor gegevensbescherming gelden (krachtens het Verdrag van Lissabon, artikel 16 van het Verdrag betreffende de werking van de Europese Unie). De harmonisatie op EU-niveau met betrekking tot de *regeling* van gegevensbescherming, betekent evenwel niet dat een overeenkomst met een derde land de *overdracht* van persoonsgegevens, ongeacht het doel, mogelijk maakt. Afhankelijk van de context en de verwerkingsvoorwaarden kunnen aangepaste waarborgen voor gegevensbescherming worden vereist op specifieke gebieden als wetshandhaving. De EDPS wenst dat bij de voorbereiding van een overeenkomst rekening wordt gehouden met de implicaties van deze verschillen tussen de invalshoeken.

III.2. **Vorm van de overeenkomst**

Het Europees institutioneel kader

29. Op korte termijn is het in elk geval van essentieel belang te bepalen binnen welke pijler zal worden onderhandeld, vooral omdat het interne regelgevingskader voor gegevensbescherming door de overeenkomst zal worden beïnvloed: de eerste pijler — dus Richtlijn 95/46/EG, met haar bijzondere regeling voor doorgifte aan derde landen — of de derde pijler, met een minder strenge regeling ([15])?

30. Zoals vermeld, is in het verslag van de HLCG het overwegende doel wetshandhaving, maar wordt ook het verzamelen van gegevens van particuliere actoren vermeld. Bovendien kunnen de doelen in bredere zin dan louter veiligheid worden geïnterpreteerd, en ook thema's als immigratie en grenscontrole omvatten, mogelijk zelfs volksgezondheid. Gezien deze onduidelijkheid is het ten sterkste aan te raden op de harmonisatie van de pijlers onder het EU-recht te wachten, zoals voorzien in het Verdrag van Lissabon, teneinde de rechtsgrond voor de onderhandelingen en de exacte rol van de Europese instellingen, meer bepaald het Europees Parlement en de Commissie, duidelijk vast te stellen.

Bindend karakter

31. Verduidelijkt moet worden of de besprekingen zullen leiden tot een memorandum van overeenstemming of een andere niet-bindende tekst, dan wel tot een bindende internationale overeenkomst.

32. De EDPS steunt de in het verslag vermelde voorkeur voor een bindende overeenkomst. Een officiële bindende overeenkomst is volgens de EDPS een onontbeerlijke voorwaarde voor de overdracht van gegevens buiten de EU, ongeacht het doel van die overdracht. Zonder de toepasselijke voorwaarden en waarborgen in een specifiek (en bindend) juridisch kader, kunnen geen gegevens worden meegedeeld aan een derde land. Met andere woorden, een memorandum van overeenstemming of een andere niet-bindende tekst kan nuttig zijn als leidraad bij de onderhandelingen over een bindende overeenkomst, maar kan de noodzaak van een bindende overeenkomst niet wegnemen.

Rechtstreekse werking

33. De bepalingen moeten even bindend zijn voor de VS, de EU en haar lidstaten.

34. Voorts moet worden verzekerd dat men op basis van de overeengekomen beginselen zijn rechten kan uitoefenen, in het bijzonder het beroepsrecht. Volgens de EDPS kan dit resultaat het best worden bereikt indien de materiële bepalingen zo worden geformuleerd dat zij rechtstreekse werking hebben voor de inwoners van de Europese Unie en in rechte kunnen worden ingeroepen. In het akkoord moet de rechtstreekse werking dus worden vastgelegd, evenals de voorwaarden voor de omzetting ervan in Europees en nationaal recht, teneinde de doeltreffendheid van de maatregelen te waarborgen.

Verhouding tot andere overeenkomsten

35. Belangrijk is voorts in hoeverre de overeenkomst op zichzelf staat, dan wel per geval moet worden aangevuld met verdere overeenkomsten betreffende specifieke gegevensuitwisseling. Het is namelijk maar de vraag of één overeenkomst, met één reeks normen, de veelheid van gegevensverwerkingsaspecten in de derde pijler zou kunnen bestrijken. Onzekerder is of zo'n overeenkomst, zonder

([14]) Verslag van de informele adviesgroep op hoog niveau inzake de toekomst van het Europees binnenlandsezakenbeleid, „Vrijheid, veiligheid, privacy — het Europese binnenlandsezakenbeleid in een open wereld", juni 2008, beschikbaar op register.consilium.europa.eu

([15]) Zie artikelen 11 en 13 van het KBGB, vermeld in punt 7 van dit advies.

aanvullende besprekingen en waarborgen, een algemene *goedkeuring* voor de doorgifte van persoonsgegevens zou kunnen inhouden, ongeacht het doel en de aard van de gegevens. Bovendien zijn overeenkomsten met derde landen niet per se permanent, omdat zij in verband kunnen staan met een bepaalde dreiging, en onderworpen kunnen zijn aan herziening en voorzien kunnen zijn van vervalclausules. Daar staat tegenover dat de gezamenlijke minimumnormen in een bindende tekst bevorderlijk kunnen zijn voor verdere besprekingen over de doorgifte van persoonsgegevens in verband met een bepaalde gegevensbank of bepaalde verwerkingen.

36. De EDPS pleit daarom voor een beperkte reeks gegevensbeschermingscriteria, die dan per geval kan worden aangevuld met specifieke bepalingen, zoals vermeld in het HLCG-verslag, in plaats van een autonome overeenkomst. Zonder zulke aanvullende specifieke bepalingen kunnen in een bepaald geval geen gegevens worden meegedeeld; zij zullen de harmonisatie van gegevensbescherming ten goede komen.

Toepassing op bestaande overeenkomsten

37. Tevens moet worden onderzocht hoe een algemene overeenkomst te combineren is met de bestaande overeenkomsten tussen de EU en de VS, die immers niet dezelfde, bindende aard hebben, bijvoorbeeld de PNR-overeenkomst (deze met de grotere mate van rechtszekerheid), de Europol- en Eurojust-overeenkomsten en de briefwisseling rond SWIFT ([16]). Zou een nieuw algemeen kader de bestaande overeenkomsten aanvullen, of deze onverlet laten en alleen op toekomstige uitwisselingen van persoonsgegevens van toepassing zijn? De EDPS is van mening dat, in het belang van de juridische samenhang, een geharmoniseerd stel regels noodzakelijk is, die op zowel bestaande als toekomstige bindende overeenkomsten inzake gegevensoverdracht van toepassing zijn en die deze overeenkomsten aanvullen.

38. Toepassing van de algemene overeenkomst op de bestaande overeenkomsten zou het voordeel hebben dat het bindende karakter van deze overeenkomsten wordt versterkt. Dit zou vooral van pas komen voor niet-bindende akkoorden zijn, zoals de briefwisseling rond SWIFT, aangezien ten minste de naleving van een stel algemene privacybeginselen zou worden opgelegd.

IV. **ALGEMENE JURIDISCHE BEOORDELING**

39. In dit hoofdstuk wordt nagegaan hoe het beschermingsniveau van een specifieke regeling of kaderregeling wordt beoordeeld, welke *benchmarks* moeten worden gebruikt en wat de basisvereisten zijn.

Passend beschermingsniveau

40. Volgens de EDPS zal een van de voornaamste resultaten van de overeenkomst moeten zijn dat de persoonsgegevens aan de Verenigde Staten kunnen worden overgedragen als autoriteiten in de VS een passend beschermingsniveau garanderen (en vice versa).

41. De EDPS is van mening dat het beschermingsniveau pas gewaarborgd kan zijn als het passende karakter echt is getest. Hij is van mening dat een algemene raamovereenkomst met een breed toepassingsgebied in de zin van het HLCG-verslag, een dergelijke test moeilijk zou doorstaan. Het passende karakter van een algemene overeenkomst kan alleen worden erkend, als het tevens wordt erkend met betrekking tot de specifieke overeenkomsten die per geval zijn gesloten.

42. Het is niet ongebruikelijk dat het door derde landen geboden beschermingsniveau wordt beoordeeld, met name door de Europese Commissie. In de eerste pijler is het passende karakter een voorwaarde voor overdracht. Het passende karakter is bij verschillende gelegenheden krachtens artikel 25 van Richtlijn 95/46/EG gemeten op basis van specifieke criteria, en bevestigd bij besluit van de Europese Commissie ([17]). De derde pijler heeft hierin niet expliciet voorzien. Meting wordt alleen voorgeschreven voor de specifieke situaties uit de artikelen 11 en 13 van het — nog niet aangenomen — kaderbesluit over de bescherming van persoonsgegevens ([18]) en wordt aan de lidstaten overgelaten.

43. In het onderhavige geval bestrijkt het toepassingsgebied de doeleinden van wetshandhaving en worden de gesprekken door de Commissie gevoerd, onder toezicht van de Raad. De context verschilt van de beoordeling van de veiligehavenbeginselen of het passende karakter van de Canadese wetgeving, en houdt meer verband met de recente PNR-onderhandelingen met de VS en met Australië, die in het juridisch kader van de derde pijler plaatsvonden. De beginselen van de HLCG zijn echter ook vermeld in het kader van het visumontheffingsprogramma, dat betrekking heeft op grenzen en immigratie, bijgevolg op de eerste pijler.

44. De EDPS pleit ervoor om bij de beoordeling van het passende karakter voortaan uit te gaan van de al bestaande ervaring op deze gebieden. Het begrip „passend karakter" zou in het kader van elke nieuwe overeenkomst

([16]) Zie voetnoot 2.

([17]) Commissiebesluiten over de passende bescherming van persoonsgegevens in derde landen, waaronder Argentinië, Canada, Zwitserland, de Verenigde Staten, Guernsey, Isle of Man en Jersey, zijn beschikbaar op http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

([18]) Beperkt tot de overdracht aan een derde land of internationaal orgaan van gegevens die een lidstaat van de bevoegde autoriteit van een andere lidstaat heeft ontvangen.

nader moeten worden uitgewerkt op basis van de criteria die al bij eerdere beoordelingen zijn gehanteerd.

Wederzijdse erkenning — wederkerigheid

45. Een tweede element van het beschermingsniveau heeft betrekking op de wederzijdse erkenning van de systemen van de VS en de EU. Volgens de HLCG is het de bedoeling dat beide partijen de doeltreffendheid van elkaars privacy- en gegevensbeschermingssystemen gaan erkennen op de gebieden die door deze beginselen worden bestreken ([19]), en een gelijke en wederzijdse toepassing van de wetgeving inzake privacy en persoonsgegevensbescherming bewerkstelligen.

46. Voor de EDPS is het duidelijk dat wederzijdse erkenning (of wederkerigheid) alleen mogelijk is indien een gepast beschermingsniveau wordt gewaarborgd. Met andere woorden, de minimumbescherming moet worden geharmoniseerd (via een beoordeling van het passende karakter, rekening houdend met de behoefte aan specifieke overeenkomsten per geval). Alleen onder deze voorwaarde kan wederkerigheid worden erkend.

47. Het eerste element waarmee rekening moet worden gehouden is de wederkerigheid van de materiële bepalingen inzake gegevensbescherming. Volgens de EDPS moet de wederkerigheid van de materiële bepalingen inzake gegevensbescherming zo worden geregeld dat enerzijds bij de gegevensverwerking op het grondgebied van de EU (en de VS) de nationale wetgeving inzake gegevensbescherming ten volle wordt gerespecteerd, en anderzijds de gegevensverwerking buiten het land van oorsprong die binnen het toepassingsgebied van de overeenkomst valt, gebeurt volgens de gegevensbeschermingsbeginselen uit de overeenkomst.

48. Het tweede element is de wederkerigheid van de beroepsmogelijkheden. Europese burgers wier persoonsgegevens in de Verenigde Staten worden verwerkt, moeten — ongeacht de wetgeving die van toepassing is — over voldoende beroepsmogelijkheden beschikken, maar ook de Europese Unie en haar lidstaten moeten gelijke rechten bieden aan de Amerikaanse burgers.

49. Het derde element is dat de wetshandhavingsautoriteiten op basis van wederkerigheid toegang moeten hebben tot de persoonsgegevens. Dit houdt in dat, als een overeenkomst de Amerikaanse autoriteiten toegang geeft tot gegevens uit de Europese Unie, de autoriteiten van de EU evenzeer toegang moeten krijgen tot gegevens uit de VS. De wederkerigheid mag de doeltreffendheid van de bescherming niet aantasten. Deze voorwaarde moet absoluut vervuld zijn, willen de gegevens „trans-Atlantisch" toegankelijk worden gesteld voor de wetshandhavingsautoriteiten. Concreet betekent dit dat:

— de Amerikaanse autoriteiten geen rechtstreekse toegang mogen krijgen tot gegevens op het grondgebied van de EU (en vice versa); toegang mag alleen worden gegeven op indirecte basis, via een „push"-systeem;

— deze toegang onder toezicht moet staan van gegevensbeschermingsautoriteiten en de justitiële autoriteiten in het land waar de gegevensverwerking plaatsvindt;

— de toegang van de Amerikaanse autoriteiten tot gegevensbanken in de EU moet voldoen aan de materiële bepalingen inzake gegevensbescherming (zie boven) en de betrokkene over alle beroepsmogelijkheden moet beschikken.

Nauwkeurigheid van de overeenkomst

50. Het is van essentieel belang de beoordelingscriteria (passend karakter, gelijkwaardigheid, wederzijdse erkenning) precies te bepalen, aangezien dit de inhoud bepaalt in termen van nauwkeurigheid, rechtszekerheid en doeltreffendheid van de bescherming. De overeenkomst moet inhoudelijk nauwkeurig en accuraat zijn.

51. Voorts moet duidelijk zijn dat ook een specifieke overeenkomst die in een later stadium wordt gesloten, volledige en gedetailleerde gegevensbeschermingsgaranties moet bevatten in verband met het voorwerp van de beoogde uitwisseling. Zoals vermeld in de punten 35 en 36, kan alleen dit dubbele niveau van concrete gegevensbeschermingsbeginselen zorgen voor het noodzakelijke hechte verband tussen de algemene overeenkomst en de specifieke overeenkomsten.

Een model ontwikkelen voor andere derde landen

52. Bijzondere aandacht moet gaan naar de mate waarin een overeenkomst met de VS model kan staan voor overeenkomsten met andere derde landen. De EDPS merkt op dat in het eerder genoemde verslag van de Toekomstgroep, behalve de VS ook Rusland als strategische partner van de EU wordt genoemd. Voor zover de beginselen neutraal zijn en in overeenstemming met de fundamentele waarborgen van de EU, kunnen zij een nuttig precedent vormen. Specifieke kenmerken van de overeenkomst die onder meer verband houden met het juridisch kader van het ontvangende land of het doel van de overdracht zouden evenwel beletten dat de overeenkomst zonder meer wordt getransponeerd. Een even beslissende factor is de situatie van de democratie in derde landen. Verzekerd moet worden dat de overeengekomen beginselen in het ontvangende land doeltreffend worden gewaarborgd en toegepast.

Welke benchmarks moeten worden gebruikt om het beschermingsniveau te beoordelen?

53. Een impliciet of expliciet passend karakter voldoet in elk geval aan het internationale en Europese juridische kader,

([19]) Hoofdstuk A. Bindende internationale overeenkomst, blz.8.

met name de gezamenlijk overeengekomen gegevensbeschermingsgaranties, die zijn vervat in de richtsnoeren van de Verenigde Naties, Verdrag nr. 108 van de Raad van Europa en het aanvullend protocol, de OESO-richtsnoeren en het ontwerp-kaderbesluit over de bescherming van persoonsgegevens, evenals, voor eerstepijleraangelegenheden, Richtlijn 95/46/EG ([20]). Al deze teksten bevatten vergelijkbare beginselen, die algemeen zijn erkend als de kern van de persoonsgegevensbescherming.

54. Gezien de impact van een potentiële overeenkomst in de zin van het HLCG-verslag, is het des te belangrijker dat terdege rekening wordt gehouden met de bovenstaande beginselen. Een instrument dat betrekking heeft op de volledige *handhaving*ssector van een derde land, is namelijk zonder precedent. Tot dusver hebben de regelgeving over het passende karakter in de eerste pijler en overeenkomsten met derde landen in de derde pijler (Europol, Eurojust) altijd in verband gestaan met specifieke gegevensoverdracht. In het onderhavige geval zou echter, gezien de ruime doelstelling (bestrijden van strafbare feiten, nationale en openbare veiligheid, wetshandhaving aan de grenzen) en het onbekende aantal betrokken gegevensbanken, overdracht op een veel breder terrein mogelijk worden gemaakt.

Basisvereisten

55. De Groep artikel 29 heeft in een werkdocument bepaald onder welke voorwaarden persoonsgegevens aan derde landen kunnen worden overgedragen ([21]). Een overeenkomst inzake de minimumbeginselen voor privacy moet de toets der doeltreffendheid van de gegevensbeschermingswaarborgen doorstaan.

— Inzake de inhoud: de gegevensbeschermingsbeginselen moeten een hoog beschermingsniveau bieden en aan normen overeenkomstig de EU-beginselen voldoen. In dit opzicht worden de 12 in het HLCG-verslag genoemde beginselen verder geanalyseerd in hoofdstuk V van dit advies.

— Inzake de specificiteit: afhankelijk van de aard van de overeenkomst, en vooral bij officiële internationale overeenkomsten, moeten de regels en procedures voldoende gedetailleerd zijn om een doeltreffende toepassing te verzekeren.

— Inzake het toezicht: de naleving van de overeengekomen regels moet worden verzekerd door middel van specifieke controlemaatregelen, zowel intern (audits) als extern (evaluaties). Deze maatregelen moeten voor beide partijen bij de overeenkomst gelijkelijk beschikbaar zijn. Toezicht omvat maatregelen om de naleving te verzekeren op macroniveau, zoals gezamenlijke evaluaties, en op microniveau, zoals individuele beroepsmogelijkheden.

56. Naast deze drie basisvereisten moet bijzondere aandacht gaan naar de specifieke kenmerken van de persoonsgegevensverwerking in wetshandhavingsverband. Op dit gebied kunnen de grondrechten namelijk aan beperkingen onderhevig zijn. Met het oog op de consequenties hiervan voor de betrokkene, meer bepaald op de hieronder genoemde punten, moet de beperking van de persoonlijkheidsrechten met waarborgen worden omgeven.

— Transparantie: de informatie en de toegang tot persoonsgegevens kunnen in het kader van wetshandhaving worden beperkt, bijvoorbeeld omdat discretie vereist is bij het onderzoek. In dat geval worden binnen de EU ter compensatie van deze beperking van de grondrechten gewoonlijk aanvullende mechanismen ingesteld, vaak met onafhankelijke gegevensbeschermingsautoriteiten. Daarom moeten bij de overdracht van de informatie aan een derde land soortgelijke compensatiemechanismen beschikbaar zijn.

— Beroep: om de bovenstaande redenen moeten de betrokkenen hun rechten ook langs alternatieve wegen kunnen laten verdedigen, met name via een onafhankelijke toezichthouder en voor de rechter.

— Gegevensbewaring: mogelijk ontbreekt een transparante motivering van de bewaringsperiode. Dit mag de betrokkenen of toezichthoudende autoriteiten echter niet beletten om hun rechten effectief uit te oefenen.

([20]) — Richtsnoeren van de Verenigde Naties inzake computerbestanden van persoonsgegevens, aangenomen door de Algemene Vergadering op 14 december 1990 en beschikbaar op www.unhchr.ch/html/menu3/b/71.htm
— Verdrag van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, 28 januari 1981, beschikbaar op www.conventions.coe.int/treaty/en/Treaties/html/108.htm
— OESO-richtsnoeren inzake de bescherming van privacy en grensoverschrijdend verkeer van persoonsgegevens, vastgesteld op 23 september 1980, beschikbaar op http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
— Ontwerp-Kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, beschikbaar op http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371
— 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.

([21]) Werkdocument van 24 juli 1998 inzake de doorgifte van persoonsgegevens naar derde landen: toepassing van de artikelen 25 en 26 van de EU-richtlijn betreffende gegevensbescherming; WP 12.

— Verantwoordingsplicht van wetshandhavingsautoriteiten: zonder effectieve transparantie kan er geen sprake zijn van alomvattende controle door de betrokkene of de institutionele stakeholders. Gezien de gevoelige aard van de gegevens en de dwingende maatregelen die op basis van de gegevensverwerking tegen personen kunnen worden genomen, is het van essentieel belang deze controles stevig te verankeren. Verantwoordingsplicht is van doorslaggevend belang in verband met de nationale controlemaatregelen van het ontvangende land, maar ook in verband met de mogelijkheden voor herziening door het land of de regio van herkomst van de gegevens. Specifieke overeenkomsten als de PNR-overeenkomst voorzien in dergelijke herzieningsmechanismen, en de EDPS pleit er zeer sterk voor om ze ook in de algemene overeenkomst op te nemen.

V. **ANALYSE VAN DE BEGINSELEN**

Inleiding

57. In dit hoofdstuk worden de 12 beginselen uit het HLCG-verslag geanalyseerd, met inachtneming van het volgende:

— Deze beginselen tonen aan dat de VS en de EU bepaalde standpunten betreffende de beginselen delen, aangezien er gelijkenis is met de beginselen van Verdrag nr. 108.

— Desalniettemin volstaat een overeenkomst op het niveau van de beginselen niet. Een juridische tekst moet sterk genoeg zijn om de handhaving te verzekeren.

— De EDPS betreurt het dat de beginselen niet vergezeld gaan van een toelichting.

— Vooraleer nader wordt ingegaan op de beginselen, moet het vaststaan dat beide partijen dezelfde interpretatie hanteren van de gebruikte termen, bijvoorbeeld van de begrippen „persoonsgegevens" of „beschermde personen". Het zou goed zijn deze begrippen te definiëren.

1. Bepaling van het doel

58. Volgens het eerste beginsel in de bijlage bij het HLCG-verslag worden persoonsgegevens ten behoeve van gerechtvaardigde wetshandhaving verwerkt. Zoals vermeld, betekent dit voor de Europese Unie het voorkomen, opsporen, onderzoeken of vervolgen ter zake van strafbare feiten. Voor de VS reikt wetshandhaving echter verder dan strafbare feiten, en omvat zij ook „de wetshandhaving aan de grenzen, openbare en nationale veiligheid". Wat de gevolgen zijn van deze discrepantie is niet duidelijk. In het verslag staat wel dat de doeleinden in de praktijk grotendeels kunnen overeenstemmen, maar belangrijker is te weten in welke mate zij *niet* overeenstemmen. Op het gebied van wetshandhaving moet, gezien het effect van maatregelen op individuen, het doelbindingsbeginsel strikt worden nageleefd en moeten de gestelde doelen duidelijk en omschreven zijn. Ter wille van de in het verslag beoogde wederkerigheid, is het ook van essentieel belang dat de doelen onderling worden aangepast. Kortom, de interpretatie van het beginsel moet worden verduidelijkt.

2. Integriteit/kwaliteit van de gegevens

59. De EDPS is ingenomen met de bepaling dat persoonsgegevens nauwkeurig, relevant, van pas komend en volledig moeten zijn, met het oog op de rechtmatige verwerking ervan. Dit beginsel is een basisvoorwaarde voor efficiënte gegevensverwerking.

3. Noodzakelijkheid/evenredigheid

60. Het beginsel legt een duidelijk verband tussen de verzamelde gegevens en de noodzakelijkheid ervan om een wettelijk bepaald wetshandhavingsdoel te bereiken. De EDPS is ingenomen met het feit dat een wettelijke basis vereist is om de legitimiteit van de verwerking te bewijzen. Hij merkt evenwel op dat deze wettelijke basis, die weliswaar de rechtszekerheid van de verwerking ten goede komt, een wet van een derde land is en als zodanig geen rechtsgrond voor de overdracht van persoonsgegevens kan vormen ([22]). In het HLCG-verslag lijkt de legitimiteit van de wet van een derde land, *in casu* de Verenigde Staten, in principe te worden erkend. Dit moge juist zijn, omdat de VS een democratie is. Toch zou het niet opgaan voor, noch te transponeren zijn naar de betrekkingen met andere derde landen.

61. Volgens de bijlage bij het HLCG-verslag moet een overdracht van persoonsgegevens relevant, noodzakelijk en toepasselijk zijn. De EDPS benadrukt dat, met het oog op de evenredigheid, de verwerking niet al te diepgaand mag zijn en de verwerkingsmodaliteiten evenwichtig moeten zijn, met inachtneming van de rechten en belangen van de betrokkenen.

62. Daarom moet de toegang tot informatie per geval worden onderzocht, afhankelijk van de praktische behoeften in het kader van een specifiek onderzoek. Wetshandhavingsautoriteiten uit derde landen permanent toegang geven tot gegevensbanken in de EU zou niet in verhouding staan tot het doel en onvoldoende gerechtvaardigd zijn. De EDPS herinnert eraan dat zelfs met de huidige overeenkomsten inzake gegevensuitwisseling, bijv. de PNR-overeenkomst, de

([22]) Zie in het bijzonder artikel 7, onder c) en onder e) van Richtlijn 95/46/EG. In zijn advies 6/2002 van 24 oktober 2002 over de doorgifte van informatie van de passagierslijst en andere gegevens van luchtvaartmaatschappijen aan de Verenigde Staten, verklaart de groep dat het niet aanvaardbaar lijkt dat een unilateraal besluit dat door een derde land in eigen nationaal belang is genomen, zou leiden tot de stelselmatige en grootschalige doorgifte van krachtens de richtlijn beschermde gegevens.

uitwisseling van specifieke omstandigheden afhangt en binnen een beperkte tijdspanne gebeurt ([23]).

63. Volgens diezelfde logica moet ook de periode voor bewaring van gegevens worden geregeld. Gegevens mogen niet langer dan nodig worden bewaard en moeten het specifiek beschreven doel dienen. Zijn ze niet langer relevant voor dat doel, dan moeten ze worden gewist. De EDPS is sterk gekant tegen de samenstelling van *datawarehouses*, waarin informatie over niet-verdachte personen zou worden opgeslagen voor mogelijk toekomstig gebruik.

4. Beveiliging van de informatie

64. De beginselen bevatten maatregelen en procedures om de gegevens te beschermen tegen misbruik, wijziging en andere risico's, alsook een bepaling die de toegang beperkt tot gemachtigde personen. De EDPS acht dit toereikend.

65. Hieraan zou de bepaling kunnen worden toegevoegd dat logbestanden moeten worden bijgehouden van de personen die de gegevens raadplegen, om de waarborgen voor de beperking van de toegang en voor preventie van misbruik nog doeltreffender te maken.

66. Daarnaast moet worden voorzien in onderlinge informatie bij inbreuk op de beveiliging. Zo zouden ontvangers in de VS en in de EU elkaar op de hoogte moeten stellen van onwettige toegang tot de gegevens die zij ontvangen hebben. Meer verantwoordelijkheid draagt bij tot een veilige verwerking van de gegevens.

5. Bijzondere categorieën van persoonsgegevens

67. Volgens de EDPS wordt het verbod op verwerking van gevoelige informatie aanzienlijk afgezwakt doordat gevoelige gegevens waarvoor de nationale wetgeving in „passende waarborgen" voorziet, daarvan worden uitgezonderd. Juist wegens die gevoelige aard van de gegevens moeten afwijkingen op het verbod terdege en nauwkeurig worden gerechtvaardigd, met behulp van een lijst van doeleinden en omstandigheden waaronder een bepaald type van gevoelige informatie kan worden verwerkt, en met aanduiding van de hoedanigheid van de verantwoordelijken voor de verwerking van de informatie. Gewaarborgd moet worden dat gevoelige informatie op zich geen reden kan zijn om een onderzoek in te stellen. Gevoelige informatie kan in bepaalde omstandigheden beschikbaar worden gesteld, zij het alleen als aanvullende informatie over een betrokkene over wie reeds een onderzoek loopt. Deze waarborgen en voorwaarden moeten limitatief worden opgesomd.

6. Verantwoordingsplicht

68. In de punten 55-56 is reeds gezegd dat de verantwoordingsplicht van openbare lichamen die persoonsgegevens verwerken doeltreffend moet worden verzekerd, en dat in de overeenkomst moet worden aangegeven hoe dit zal gebeuren. Dit is des te belangrijker gezien het gebrek aan transparantie waarmee de verwerking van persoonsgegevens in wetshandhavingsverband vaak gepaard gaat. Het volstaat niet om — zoals nu in de bijlage — te vermelden dat overheidsinstanties verantwoording moeten afleggen, zonder daarbij uit te leggen hoe dit moet gebeuren en wat de gevolgen van de verantwoording zijn. De EDPS wenst dat deze uitleg in de tekst van de overeenkomst komt te staan.

7. Onafhankelijk en doeltreffend toezicht

69. De EDPS is voorstander van een bepaling over onafhankelijk en doeltreffend toezicht door een of meer openbare toezichthoudende autoriteiten. In deze bepaling moet worden duidelijk gemaakt wat onafhankelijkheid betekent, meer bepaald van wie de autoriteiten onafhankelijk zijn en aan wie ze verslag moeten uitbrengen. Er moeten criteria inzake de institutionele en functionele onafhankelijkheid ten opzichte van de uitvoerende en wetgevende organen worden vastgelegd. De EDPS benadrukt dat dit van essentieel belang is voor een doeltreffende naleving van de overeengekomen beginselen. De bevoegdheid van deze autoriteiten om op te treden en de wet te handhaven is ook van cruciaal belang in verband met de hierboven vermelde verantwoordingsplicht van de overheidsinstanties die persoonsgegevens verwerken. De betrokkenen moeten op de hoogte worden gebracht van het bestaan en de bevoegdheden van deze autoriteiten, zodat zij hun rechten kunnen uitoefenen. Dit geldt vooral indien, afhankelijk van de context van de verwerking, verschillende autoriteiten bevoegd zijn.

70. Voorts pleit de EDPS ervoor dat de overeenkomst ook in samenwerkingsmechanismen tussen de toezichthoudende autoriteiten voorziet.

8. Individuele toegang en rectificatie

71. Er zijn specifieke garanties nodig voor toegang en rectificatie in wetshandhavingsverband. In die zin is de EDPS ingenomen met het beginsel dat eenieder toegang krijgt (moet krijgen) tot zijn/haar persoonsgegevens en rectificatie en/of schrapping van zijn/haar persoonsgegevens kan (moet kunnen) vragen. Er bestaat evenwel nog onduidelijkheid over de definitie van persoon (alle betrokkenen moeten worden beschermd, niet alleen de burgers van het betreffende land), en over de voorwaarden waaronder personen bezwaar kunnen aantekenen tegen de verwerking van hun gegevens. Ook moeten de „geëigende gevallen" waarin al dan niet bezwaar kan worden aangetekend nauwkeuriger

([23]) Deze overeenkomst verstrijkt en is niet langer van kracht zeven jaar na de datum van ondertekening ervan, tenzij de partijen deze met wederzijdse instemming vervangen.

worden omschreven. Het moet de betrokkenen duidelijk zijn in welke omstandigheden — bijv. afhankelijk van het soort autoriteit, het type onderzoek of andere criteria — zij hun rechten zullen kunnen uitoefenen.

72. Indien het om gerechtvaardigde redenen niet mogelijk is rechtstreeks bezwaar aan te tekenen tegen een verwerking, moet wel een indirecte verificatie beschikbaar zijn via de onafhankelijke autoriteit die toeziet op de verwerking.

9. Transparantie en kennisgeving

73. De EDPS benadrukt nogmaals hoe belangrijk doeltreffende transparantie is om de betrokkenen hun rechten te laten uitoefenen en bij te dragen tot de algemene verantwoordingsplicht van overheidsinstanties die persoonsgegevens verwerken. Hij steunt de opgestelde beginselen en benadrukt dat algemene *en* individuele kennisgeving aan de betrokkene noodzakelijk is. Dit wordt weergegeven in het beginsel in punt 9 van de bijlage.

74. In het verslag in hoofdstuk 2, B („Overeengekomen beginselen") staat echter vermeld dat dit in de VS „(een combinatie van) de publicatie in het *Federal Register*, individuele kennisgeving en openbaarmaking bij gerechtelijke procedures" kan omvatten. Het moet duidelijk zijn dat een bekendmaking in een publicatieblad te weinig garantie biedt dat de betrokkene voldoende geïnformeerd is. De EDPS herinnert eraan dat individuele kennisgeving, in een voor de betrokkene gemakkelijk te begrijpen vorm en taal, noodzakelijk is.

10. Beroepsmogelijkheden

75. Om zijn rechten effectief te kunnen uitoefenen, moet men een klacht kunnen indienen bij een onafhankelijke gegevensbeschermingsautoriteit, en over een voorziening in rechte beschikken voor een onafhankelijke en onpartijdige instantie. Beide beroepsmogelijkheden moeten in dezelfde mate beschikbaar zijn.

76. Toegang tot een onafhankelijke gegevensbeschermingsautoriteit is noodzakelijk, omdat dit een soepele en minder dure bijstand mogelijk maakt in een context — wetshandhaving — die voor de burger veeleer ondoorzichtig is. Ook kunnen de gegevensbeschermingsautoriteiten de betrokkene bijstand verstrekken wanneer deze in uitzonderlijke gevallen zijn persoonsgegevens niet rechtstreeks heeft kunnen raadplegen en toch zijn recht op toegang wil uitoefenen.

77. Toegang tot de rechter is een extra en onontbeerlijke garantie dat de betrokkene beroep kan aantekenen bij een instantie die deel uitmaakt van het democratische systeem en volledig losstaat van de overheidsinstellingen die zijn gegevens verwerken. Een dergelijke doeltreffende voorziening voor een gerecht beschouwt het Europees Hof van Justitie ([24]) als „van wezenlijk belang om de particulier een doeltreffende bescherming van zijn recht te waarborgen. (…) (Het) vormt een algemeen beginsel van Gemeenschapsrecht dat voortvloeit uit het constitutionele erfgoed dat alle lidstaten gemeen hebben en dat eveneens is neergelegd in de artikelen 6 en 13 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden.". Ook in artikel 22 van Richtlijn (EG) nr. 95/46/EG en in artikel 47 van het EU-handvest van de grondrechten wordt de mogelijkheid van voorziening in rechte, onverminderd een administratieve voorziening, expliciet vermeld.

11. Geautomatiseerde individuele besluiten

78. De EDPS is ingenomen met de bepaling inzake toereikende waarborgen bij de geautomatiseerde verwerking van persoonsgegevens. Hij merkt op dat met een gezamenlijk begrip van een „significant negatief effect voor de belangen van de persoon" de toepassingsvoorwaarden van dit beginsel zouden worden verduidelijkt.

12. Verdere overdracht

79. De voorwaarden voor verdere overdracht zijn niet overal even duidelijk. Met betrekking tot overdracht die moet voldoen aan de internationale regelingen en overeenkomsten tussen het verzendende en het ontvangende land, moet worden verduidelijkt of dit slaat op overeenkomsten tussen de twee landen van de oorspronkelijke overdracht, of tussen de twee landen die bij de verdere overdracht zijn betrokken. Volgens de EDPS zijn overeenkomsten tussen de twee landen die de eerste overdracht hebben aangevat sowieso noodzakelijk.

80. De EDPS merkt tevens op dat de definitie van „rechtmatig algemeen belang", waardoor de verdere overdracht wordt gerechtvaardigd, zeer ruim is. Het toepassingsgebied van algemene veiligheid blijft onduidelijk, en de verlenging van overdracht bij schending van de beroepscode van een gereglementeerd beroep lijkt niet gerechtvaardigd en excessief in wetshandhavingsverband.

VI. **CONCLUSIE**

81. De EDPS is ingenomen met de gezamenlijke inspanningen van de autoriteiten van de EU en de VS op het gebied van wetshandhaving, waar gegevensbescherming van cruciaal belang is. Hij wenst evenwel te benadrukken dat dit een complex gegeven is, met name wat het precieze toepassingsgebied en de vorm betreft, en dat daarom een nauwkeurige en grondige analyse geboden is. De impact van

([24]) Zaak 222/84 *Johnston* [1986], Jurispr. blz. 1651; zaak 222/86 *Heylens* [1987], Jurispr. blz. 4097; zaak C-97/91, Borelli [1992] Jurispr. blz. I-6313.

een trans-Atlantisch instrument voor gegevensbescherming op het bestaande juridische kader en de gevolgen ervan voor de burger moeten terdege worden onderzocht.

82. De EDPS roept op tot meer duidelijkheid en concrete bepalingen, met name wat de volgende aspecten betreft:

— verduidelijking van de vorm van de overeenkomst, die, om voldoende rechtszekerheid te bieden, juridisch bindend zou moeten zijn;

— grondige beoordeling van het passende karakter, op basis van essentiële vereisten voor de inhoud, de specificiteit en het toezicht van de regeling. De EDPS vindt dat het passende karakter van de algemene overeenkomst alleen kan worden beoordeeld in combinatie met passende specifieke overeenkomsten per geval;

— een begrensd toepassingsgebied, met een duidelijke en gezamenlijke definitie van de wetshandhavingsdoeleinden;

— precisering van de modaliteiten voor het betrekken van particuliere entiteiten bij gegevensoverdracht;

— naleving van het evenredigheidsbeginsel, wat inhoudt dat de gegevens worden uitgewisseld per geval, als er een concrete behoefte bestaat;

— krachtig toezicht, alsook beroepsmogelijkheden voor de betrokkenen, met inbegrip van administratieve en rechtsmiddelen;

— doeltreffende maatregelen teneinde te verzekeren dat alle betrokkenen, ongeacht hun nationaliteit, hun rechten kunnen uitoefenen;

— inschakeling onafhankelijke gegevensbeschermingsautoriteiten, met name voor het toezicht en de bijstand aan de betrokkenen.

83. De EDPS benadrukt dat de beginselen niet overhaast mogen worden uitgewerkt, aangezien dit een averechts effect zou sorteren. De beste optie zou dus de ontwikkeling van een routekaart voor een overeenkomst in een later stadium zijn.

84. De EPDS roept ook op tot meer transparantie bij de uitwerking van gegevensbeschermingsbeginselen. Alleen als alle stakeholders, ook het Europees Parlement, hierbij worden betrokken, kan de overeenkomst met een democratisch debat de noodzakelijke steun en erkenning verwerven.

Gedaan te Brussel, 11 november 2008.

Peter HUSTINX

Europese Toezichthouder voor gegevensbescherming