Advies van de Europese Toezichthouder voor gegevensbescherming over de mededeling van de Commissie aan het Europees Parlement en de Raad betreffende een ruimte van vrijheid, veiligheid en recht ten dienste van de burger

(2009/C 276/02)

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, met name op artikel 41,

BRENGT HET VOLGENDE ADVIES UIT:

I. INLEIDING

1. De Commissie heeft op 10 juni 2009 haar mededeling aan het Europees Parlement en de Raad betreffende een ruimte van vrijheid, veiligheid en recht ten dienste van de burger aangenomen ([1]). Overeenkomstig artikel 41 van Verordening (EG) nr. 45/2001 brengt de EDPS daarover dit advies uit.

2. Voorafgaand aan de aanneming van haar mededeling heeft de Commissie de EDPS geraadpleegd per brief van 19 mei 2009. De EDPS heeft op 20 mei 2009 op deze raadpleging gereageerd met informele opmerkingen ter verdere verbetering van de tekst van de mededeling van de Commissie. Voorts heeft de EDPS actief bijgedragen aan de brief van 14 januari 2009 van de Groep politie en justitie over het meerjarenprogramma op het gebied van justitie, vrijheid en recht ([2]).

3. De mededeling benadrukt (onder punt 1) het volgende: „De Unie heeft een nieuw meerjarenprogramma nodig, dat zich, uitgaande van de geboekte vorderingen en de bestaande tekortkomingen, met ambitie op de toekomst richt. In dit nieuwe programma moeten de prioriteiten voor de komende vijf jaar worden geformuleerd.". Dit meerjarenprogramma (al bekend als het programma van Stockholm) zal de follow-up zijn van het programma van Tampere en het Haags programma, die voor een sterke politieke impuls op het gebied van vrijheid, veiligheid en recht hebben gezorgd.

4. De mededeling moet de basis van dit nieuwe meerjarenprogramma worden. De EDPS wijst er in dit verband op dat ofschoon de meerjarenprogramma's op zich geen bindende instrumenten zijn, zij toch aanzienlijke gevolgen hebben op het beleid dat de instellingen op het betrokken gebied zullen ontwikkelen, aangezien vele van de concrete wetgevende en niet-wetgevende maatregelen eruit voortvloeien.

5. De mededeling zelf moet vanuit dat oogpunt worden bekeken. Het is de volgende stap in een debat dat min of meer begonnen is met de presentatie in juni 2008 van twee rapporten van de zogenaamde Toekomstgroepen die het voorzitterschap van de Raad had opgezet om ideeën aan te reiken: „Vrijheid, veiligheid, privacy — het Europese binnenlandsezakenbeleid in een open wereld" ([3]) en „Voorgestelde oplossingen voor het toekomstige justitieprogramma van de EU" ([4]).

II. KERNPUNTEN VAN HET ADVIES

6. Dit advies is niet alleen een reactie op de mededeling, maar ook een bijdrage van de EDPS tot het meer algemene debat over de toekomst van de ruimte van vrijheid, veiligheid en recht, dat moet uitmonden in een nieuw strategisch werkprogramma (het programma van Stockholm), zoals het Zweedse voorzitterschap van de EU heeft aangekondigd ([5]). In dit advies zal ook een aantal gevolgen van de mogelijke inwerkingtreding van het Verdrag van Lissabon aan de orde komen.

7. Na een uiteenzetting over de belangrijkste perspectieven van het advies in deel III, zal in deel IV een algemene evaluatie van de mededeling worden gemaakt.

8. Deel V gaat over de vraag hoe moet worden gereageerd op de behoefte aan een permanente eerbiediging van de bescherming van de persoonlijke levenssfeer en van persoonsgegevens in een context waarin de uitwisseling van persoonsgegevens toeneemt. De nadruk zal liggen op punt 2.3 van de mededeling, over de bescherming van persoonsgegevens en de persoonlijke levenssfeer, en meer in het algemeen over de noodzaak van meer wetgevende en niet-wetgevende maatregelen om het kader voor gegevensbescherming te verbeteren.

([1]) COM(2009) 262 definitief (hierna „de mededeling").

([2]) Niet bekendgemaakt. De Groep politie en justitie (GPJ) is opgericht door de Europese conferentie van gegevensbeschermingsfunctionarissen om de standpunten van de Conferentie op het gebied van wetshandhaving voor te bereiden en in dringende gevallen namens haar op te treden.

([3]) Document nr. 11657/08 van de Raad. Hierna „het Rapport binnenlandsezakenbeleid".

([4]) Document nr. 11549/08 van de Raad (hierna „het Rapport justitie").

([5]) Het EU-werkprogramma van de regering, zie http://www.regeringen.se

9. In deel VI worden de behoefte aan en de mogelijkheden voor opslag, toegang en uitwisseling van informatie als instrumenten voor wetshandhaving besproken of, zoals het in de mededeling is geformuleerd, voor „een Europa dat bescherming biedt". In punt 4 van de mededeling komt een aantal doelstellingen van de informatiestroom en technische instrumenten aan bod, met name in punt 4.1.2 (Informatiebeheer), punt 4.1.3 (Inzet van de noodzakelijke technologische hulpmiddelen) en punt 4.2.3.2 (Informatiesystemen). De ontwikkeling van een Europees informatiemodel (zie punt 4.1.2) kan in dat verband als het meest ambitieuze voorstel worden beschouwd. In het advies van de EDPS wordt dat voorstel grondig geanalyseerd.

10. In deel VII wordt kort stilgestaan bij een specifiek thema dat binnen de ruimte van vrijheid, veiligheid en recht van belang is voor gegevensbescherming, namelijk de toegang tot justitie en e-Justice.

III. DE PERSPECTIEVEN VAN HET ADVIES

11. In dit advies is de noodzaak van de bescherming van de grondrechten de belangrijkste invalshoek voor de analyse van de mededeling, en meer in het algemeen de toekomst van de ruimte van vrijheid, veiligheid en recht, zoals die door een nieuw meerjarenprogramma gestalte wordt gegeven. Voorts bouwt het verder op de bijdragen van de EDPS aan de ontwikkeling van het EU-beleid ter zake, hoofdzakelijk in zijn rol als raadgever. De EDPS heeft tot dusverre meer dan dertig adviezen en opmerkingen aangenomen over initiatieven die voortvloeien uit het Haags programma, die allemaal beschikbaar zijn op de website van de EDPS.

12. Bij deze evaluatie van de mededeling zal de EDPS met name rekening houden met de volgende vier perspectieven, die van belang zijn voor de toekomst van de ruimte van vrijheid, veiligheid en recht. Al deze perspectieven spelen ook in de mededeling een hoofdrol.

13. Het eerste perspectief is de exponentiële groei van digitale informatie over burgers ingevolge de ontwikkeling van de informatie- en communicatietechnologieën ([6]). De samenleving evolueert naar wat vaak de „gecontroleerde samenleving" wordt genoemd, waar elke transactie en nagenoeg elke beweging van de burger een digitaal spoor kan creëren. Het zogenaamde „internet der dingen" en de „intelligente omgeving" ontwikkelen zich snel door het gebruik van RFID-tags. Steeds vaker wordt gebruik gemaakt van gedigitaliseerde kenmerken van het menselijk lichaam (biometrische gegevens). Dit leidt tot een steeds verdere aaneengeschakelde wereld waarin de openbare veiligheidsdiensten toegang kunnen hebben tot omvangrijke hoeveelheden potentieel nuttige informatie, hetgeen de levens van de betrokkenen rechtstreeks kan beïnvloeden.

14. Internationalisering vormt het tweede perspectief. In het digitale tijdperk stopt de informatie-uitwisseling niet aan de buitengrenzen van de Europese Unie, maar is er tegelijk een groeiende behoefte aan internationale samenwerking op het gehele gebied van EU-activiteiten in de ruimte van vrijheid, veiligheid en recht: terrorismebestrijding, politiële en justitiële samenwerking, civielrechtelijke kwesties en grenscontrole zijn slechts een paar voorbeelden.

15. Het gebruik van gegevens voor wetshandhavingsdoelstellingen vormt het derde perspectief: recente maatschappelijke dreigingen, al dan niet in samenhang met terrorisme, hebben geleid tot (vergen) meer mogelijkheden voor rechtshandhavingsinstanties om persoonsgegevens te verzamelen, op te slaan en uit te wisselen. In veel gevallen zijn daarbij particuliere partijen actief betrokken, zoals onder meer de richtlijn gegevensbewaring ([7]) en de diverse instrumenten in verband met PNR ([8]) aantonen.

16. Het vrije verkeer is het vierde perspectief. De geleidelijke ontwikkeling van een ruimte van vrijheid, veiligheid en recht vereist dat de binnengrenzen en de mogelijke hinderpalen voor het vrije verkeer in die ruimte verder worden weggenomen. Nieuwe instrumenten op dit gebied mogen in geen geval tot het herinvoeren van belemmeringen leiden. Het vrije verkeer in de huidige context omvat aan de ene kant het vrije personenverkeer en aan de andere kant het vrije verkeer van (persoons)gegevens.

17. Deze vier perspectieven tonen aan dat de context waarin informatie wordt gebruikt, snel aan het veranderen is. In die context kan er geen twijfel bestaan over het belang van een sterk mechanisme voor de bescherming van de grondrechten van de burgers, in het bijzonder wat de persoonlijke levenssfeer en gegevensbescherming betreft. Om die reden heeft de EDPS de noodzaak van bescherming als belangrijkste invalshoek voor deze analyse gekozen, zoals vermeld in punt 11.

([6]) Het „Rapport binnenlandsezakenbeleid" spreekt in dit verband van een „digitale tsunami".

([7]) 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.

([8]) Zie bijvoorbeeld de 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 ministerie van Binnenlandse veiligheid van de Verenigde Staten van Amerika (PNR-overeenkomst 2007), PB L 204 van 4.8.2007, blz. 18, en het voorstel voor een kaderbesluit van de Raad over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor wetshandhavingsdoeleinden, COM(2007) 654 def.

IV. **ALGEMENE BEOORDELING**

18. De mededeling en het programma van Stockholm zijn opgesteld om de voornemens van de EU voor de komende vijf jaar te verduidelijken, met mogelijke gevolgen op zelfs langere termijn. De EDPS stelt vast dat de mededeling geschreven is op een zogenaamde „Lissabonneutrale" manier. De EDPS begrijpt terdege waarom de Commissie voor die aanpak heeft gekozen, maar betreurt dat de Commissie niet ten volle profijt heeft getrokken van de bijkomende mogelijkheden die het Verdrag van Lissabon biedt. Het Verdrag van Lissabon als invalshoek zal in dit advies meer nadruk krijgen.

19. De mededeling bouwt voort op de resultaten van de EU-maatregelen in de ruimte van vrijheid, veiligheid en recht van de afgelopen jaren. Die resultaten worden aangestuurd door gebeurtenissen; de nadruk ligt op maatregelen die de bevoegdheden van de wetshandhavingsdiensten uitbreiden en die voor de burger een ingrijpend karakter hebben. Dit is zeker het geval op de gebieden waar persoonsgegevens intensief worden gebruikt en uitgewisseld, en die daarom van cruciaal belang zijn voor gegevensbescherming. De resultaten worden aangestuurd door gebeurtenissen, getuige de sterke stimulans die externe gebeurtenissen zoals 9/11 en de bomaanslagen in Madrid en Londen, aan het wetgevingsproces hebben gegeven. De overdracht van persoonsgegevens aan de Verenigde Staten bijvoorbeeld, kan beschouwd worden als een gevolg van 9/11 ([9]) en de bomaanslagen in Londen hebben tot Richtlijn 2006/24/EG ([10]) inzake gegevensbewaring geleid. De klemtoon lag op ingrijpender maatregelen aangezien de EU-wetgever zich concentreerde op maatregelen die het gebruik en de uitwisseling van gegevens vergemakkelijken terwijl het debat over maatregelen ter bescherming van persoonsgegevens een minder dringend karakter kreeg. De belangrijkste beschermingsmaatregel, die na drie jaar van besprekingen in de Raad is aangenomen, is Kaderbesluit 2008/977/JBZ over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken ([11]). Dit heeft een niet geheel bevredigend Kaderbesluit opgeleverd (zie de punten 29 en 30).

20. De ervaring van de afgelopen jaren toont aan dat er behoefte is aan bezinning over de gevolgen voor de wetshandhavingsdiensten en voor de Europese burgers, voordat nieuwe instrumenten worden aangenomen. Tijdens die bezinning moet middels periodieke evaluaties adequate aandacht worden besteed aan de gevolgen voor de persoonlijke levenssfeer en aan de doeltreffendheid van de wetshandhaving; in eerste instantie wanneer nieuwe instrumenten worden voorgesteld en besproken, maar ook nadat die instrumenten zijn ingevoerd. Die bezinning is ook van essentieel belang voordat met een nieuw meerjarenplan belangrijke initiatieven voor de nabije toekomst hun beslag krijgen.

21. Het verheugt de EDPS dat in de mededeling de bescherming van de grondrechten, en in het bijzonder de bescherming van persoonsgegevens, erkend wordt als een van de belangrijkste vraagstukken voor de toekomst van de ruimte van vrijheid, veiligheid en recht. In punt 2 van de mededeling wordt de EU gekenschetst als een unieke ruimte voor de op gemeenschappelijke waarden gebaseerde bescherming van de grondrechten. Het is ook goed dat in de mededeling de toetreding tot het Europees Verdrag voor de Rechten van de Mens als prioriteit — zelfs als eerste prioriteit — wordt aangemerkt. De toetreding is een belangrijke stap om een harmonieus en coherent stelsel ter bescherming van de grondrechten te waarborgen. Ten slotte, maar daarom niet minder belangrijk: gegevensbescherming heeft in de mededeling een prominente plaats gekregen.

22. Dat in de mededeling dit accent wordt gelegd, wijst op de sterke wil om de bescherming van de rechten van de burgers te waarborgen en daarbij een meer evenwichtige aanpak te volgen. Regeringen hebben passende instrumenten nodig om de veiligheid van de burger te waarborgen, maar in onze Europese samenleving moeten zij de grondrechten van de burgers ten volle eerbiedigen. Wil de Europese Unie ten dienste staan van de burger ([12]), dan moet zij dat evenwicht bewaken.

23. De EDPS is van oordeel dat in de mededeling terdege rekening is gehouden met de noodzaak van dat evenwicht, onder meer met de noodzaak van de bescherming van persoonsgegevens. De mededeling onderkent dat er behoefte is aan een accentverschuiving. Dat is belangrijk, aangezien het beleid in de ruimte van vrijheid, veiligheid en recht het geleidelijk ontstaan van een gecontroleerde samenleving niet moet bevorderen. De EDPS verwacht van de Raad dat hij hetzelfde standpunt inneemt in het programma van Stockholm, mede door de strekking van punt 25 te onderschrijven.

24. Dit is des te belangrijker aangezien de ruimte van vrijheid, veiligheid en recht een ruimte is die „vorm geeft aan de levensomstandigheden van de burger, in het bijzonder aan de particuliere ruimte van hun eigen verantwoordelijkheid, en van hun persoonlijke en sociale veiligheid, die beschermd is door de grondrechten," zoals recentelijk werd benadrukt door het Duitse Grondwettelijk Hof in zijn arrest van 30 juni 2009 in verband met het Verdrag van Lissabon ([13]).

([9]) De PNR-Overeenkomst van 2007, en de voorgangers daarvan, als bedoeld in de vorige voetnoot.

([10]) 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. Ofschoon artikel 95 EG de rechtsgrondslag is, was deze richtlijn een onmiddellijk antwoord op de bomaanslagen in Londen.

([11]) Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, PB L 350 van 30.12.2008, blz. 60.

([12]) Zie titel van de mededeling.

([13]) Persbericht nr. 72/2009 van 30 juni 2009 van het Duitse Grondwettelijk Hof, punt 2, onder c).

25. De EDPS benadrukt dat in een dergelijke ruimte:

— informatie tussen de autoriteiten van de lidstaten, ook tussen de betrokken Europese organen of databanken, moet worden uitgewisseld op basis van passende en doeltreffende mechanismen die de grondrechten van de burgers volledig eerbiedigen en wederzijds vertrouwen waarborgen;

— dit vereist niet alleen dat informatie beschikbaar is en dat de lidstaten elkaars rechtsstelsels (en dat van de EU) wederzijds erkennen, maar het vergt tevens een harmonisering van de normen ter bescherming van de informatie, bijvoorbeeld, maar niet alleen, door middel van een gemeenschappelijk kader voor gegevensbescherming;

— die gemeenschappelijke normen mogen niet alleen van toepassing zijn in gevallen met een grensoverschrijdende dimensie. Wederzijds vertrouwen kan alleen bestaan op basis van solide normen die altijd geëerbiedigd worden, zonder dat het risico bestaat dat zij niet meer worden toegepast zodra de grensoverschrijdende dimensie niet of niet langer aanwezig is. Afgezien daarvan, en met name zodra het gebruik van informatie aan de orde is, zijn verschillen tussen interne en „grensoverschrijdende" gegevens in de praktijk niet werkbaar ([14]).

V. INSTRUMENTEN VOOR GEGEVENSBESCHERMING

V.1. Naar een alomvattende regeling voor gegevensbescherming

26. De EDPS onderschrijft de strategische aanpak om gegevensbescherming in de mededeling een prominente plaats te geven. Vele initiatieven in de ruimte van vrijheid, veiligheid en recht zijn immers gebaseerd op het gebruik van persoonsgegevens, en een goede gegevensbescherming is van cruciaal belang voor hun succes. Bescherming van de persoonlijke levenssfeer en gegevensbescherming is niet alleen een wettelijke verplichting die in toenemende mate op EU-niveau wordt erkend, maar ook een zaak die van wezenlijk belang is voor de Europese burgers, zoals de resultaten van de Eurobarometer hebben aangetoond ([15]). Daarnaast is het beperken van de toegang tot persoonsgegevens van cruciaal belang om het vertrouwen in wetshandhavinginstanties te waarborgen.

27. In punt 2.3 van de mededeling staat dat een integrale regeling voor de bescherming van persoonsgegevens die geldt voor alle bevoegdheidsgebieden van de Unie ([16]), noodzakelijk is. De EDPS staat pal achter deze doelstelling, los van het feit of het Verdrag van Lissabon al dan niet in werking treedt. Hij merkt ook op dat een dergelijke regeling niet noodzakelijk neerkomt op één juridisch kader voor elke vorm van verwerking. De pijlerstructuur en het feit dat — althans in de eerste pijler — de bescherming van door de Europese instellingen verwerkte gegevens op een afzonderlijke rechtsgrond stoelt (artikel 286 EG), beperken de mogelijkheden om met de huidige verdragen één algemeen rechtskader voor elke vorm van verwerking aan te nemen. De EDPS wijst er evenwel op dat een aantal verbeteringen kan worden aangebracht door de mogelijkheden van de huidige verdragen ten volle te gebruiken, zoals de Commissie reeds heeft gesteld in haar mededeling „Uitvoering van het Haags programma: koersbepaling" ([17]). Na de inwerkingtreding van het Verdrag van Lissabon zal artikel 16 VWEU een voldoende rechtsgrondslag vormen voor één alomvattend rechtskader voor alle verwerkingen.

28. De EDPS wijst erop dat het van wezenlijk belang is om — in ieder geval — de samenhang binnen het rechtskader van gegevensbescherming te waarborgen, waar nodig middels harmonisering en consolidering van de verschillende wetsinstrumenten die in de ruimte van vrijheid, veiligheid en recht van toepassing zijn.

In het kader van de bestaande verdragen

29. Onlangs werd een eerste stap gezet met de aanneming van Kaderbesluit 2008/977/JBZ van de Raad ([18]). Dat rechtsinstrument kan echter niet als alomvattend kader worden aangemerkt, hoofdzakelijk omdat de bepalingen ervan niet algemeen toepasselijk zijn. Zij zijn niet van toepassing op binnenlandse situaties, wanneer persoonsgegevens afkomstig zijn uit de lidstaat die ze gebruikt. Die beperking trekt ongetwijfeld een wissel op de meerwaarde van het kaderbesluit, tenzij alle lidstaten zouden besluiten de binnenlandse situaties onder de nationale uitvoeringswetgeving te laten vallen, wat niet erg waarschijnlijk is.

30. Een tweede reden waarom de EDPS verwacht dat Kaderbesluit 2008/977/JBZ op lange termijn geen bevredigend kader voor de bescherming van persoonsgegevens in een ruimte van vrijheid, veiligheid en recht biedt, is dat diverse essentiële bepalingen ervan niet stroken met Richtlijn 95/46/EG. In het kader van de huidige verdragen zou een tweede stap erin kunnen bestaan het toepassingsgebied te verruimen en het kaderbesluit aan Richtlijn 95/46/EG aan te passen.

31. Ook het ontwikkelen van een duidelijke en op de lange termijn gerichte visie zou een aanzet kunnen geven tot het tot stand brengen van een alomvattende regeling voor de bescherming van persoonsgegevens. Een dergelijke visie zou kunnen aangeven hoe het verzamelen en uitwisselen van gegevens — evenals het gebruik van bestaande gegevensbestanden — en tegelijkertijd de gegevensbeschermingswaarborgen algemeen en coherent kunnen

([14]) De EDPS heeft dat laatste punt nader uitgewerkt in het advies van 19 december 2005 over het voorstel voor een kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken (COM(2005) 475 def.), PB C 47 van 25.2.2006, blz. 27, punten 30 tot en met 32.

([15]) Data Protection in the European Union — Citizens' perceptions — Analytical report, Flash Eurobarometer Series 225, Jan. 2008, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf

([16]) Zie ook de prioritaire aangelegenheden in de mededeling.

([17]) COM(2006) 331 def. van 28 juni 2006.

([18]) Zie voetnoot 11.

worden omschreven. Die visie moet ervoor zorgen dat nutteloze overlapping en verdubbeling van instrumenten (en dus ook van het verwerken van persoonsgegevens) worden vermeden. Voorts moet zij de samenhang van het EU-beleid op dit gebied en het vertrouwen in de manier waarop de overheid met de gegevens van burgers omgaat ten goede komen. De EDPS beveelt de Raad aan om in het programma van Stockholm de noodzaak van een duidelijke langetermijnvisie te vermelden.

32. Een andere aanbeveling van de EDPS betreft het evalueren en in een breder verband bekijken van de maatregelen die op dit gebied reeds genomen zijn en van de concrete uitvoering en de effectiviteit van die maatregelen. Bij die evaluatie moet terdege rekening worden gehouden met gevolgen voor de persoonlijke levenssfeer en de effectiviteit voor de rechtshandhaving. Mocht uit die evaluaties blijken dat bepaalde maatregelen niet de beoogde resultaten opleveren of niet evenredig zijn met de nagestreefde doelen, dan verdient het aanbeveling de volgende stappen te overwegen:

— als eerste stap, wijziging of intrekking van de maatregelen voor zover het niet voldoende gerechtvaardigd lijkt dat zij een concrete meerwaarde opleveren voor de rechtshandhavingsinstanties en voor de Europese burgers;

— als tweede stap, evaluatie van de mogelijkheden om de uitvoering van de bestaande maatregelen te verbeteren;

— pas als derde stap, voorstellen van nieuwe wetgevingsmaatregelen, indien het waarschijnlijk is dat die nieuwe maatregelen nodig zijn om de nagestreefde doelen te verwezenlijken. Er moeten alleen nieuwe instrumenten worden aangenomen als zij een duidelijke en concrete meerwaarde hebben voor de rechtshandhavingsinstanties en voor de Europese burgers.

De EDPS beveelt aan om in het programma van Stockholm gewag te maken van een systeem van evaluatie van bestaande maatregelen.

33. En ten slotte moet er speciale nadruk worden gelegd op het beter uitvoeren van de bestaande waarborgen, overeenkomstig de mededeling van de Commissie over de follow-up van het Werkprogramma voor een betere toepassing van de Richtlijn gegevensbescherming ([19]) en de suggesties van de EDPS in zijn advies over die mededeling ([20]). Helaas beschikt de Commissie in de derde pijler niet over de mogelijkheid om inbreukprocedures in te leiden.

In het kader van het Verdrag van Lissabon

34. Het Verdrag van Lissabon biedt perspectief op een volwaardig alomvattend kader voor gegevensbescherming. Artikel 16, lid 2, van het Verdrag betreffende de werking van de Europese Unie bepaalt dat de Raad en het Europees Parlement de voorschriften betreffende gegevensbescherming door de instellingen, organen en instanties van de Unie, door de lidstaten bij activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, en door particuliere partijen.

35. De EDPS vat de beklemtoning in de mededeling van een alomvattende regeling voor gegevensbescherming op als een ambitie van de Commissie om te komen met een wettelijk kader dat op alle verwerkingsactiviteiten van toepassing is. Hij staat volledig achter die ambitie, die de innerlijke samenhang van het systeem versterkt, rechtszekerheid biedt en daardoor de bescherming verbetert. Met name zou daardoor in de toekomst de scheidslijn tussen de pijlers gemakkelijker kunnen worden getrokken wanneer in de particuliere sector voor commerciële doeleinden verzamelde gegevens later gebruikt worden voor de rechtshandhaving. Die scheidslijn tussen de pijlers geeft niet volledig de werkelijkheid weer, zoals wordt aangetoond door de belangrijke arresten van het Hof van Justitie inzake PNR-gegevens ([21]) en bewaring van gegevens ([22]).

36. De EDPS geeft in overweging om de argumenten voor een alomvattende regeling voor gegevensbescherming in het programma van Stockholm over te nemen. Dan wordt duidelijk dat een dergelijk systeem niet louter de voorkeur verdient, maar een noodzaak is vanwege de veranderende praktijken in het gebruik van gegevens. Hij beveelt aan om in het programma van Stockholm als prioriteit op te nemen dat er een nieuw wetgevingskader moet komen, en dat daarvoor onder meer Kaderbesluit 2008/977/JBZ wordt vervangen.

37. De EDPS onderstreept dat de notie van een alomvattend systeem voor gegevensbescherming op basis van een algemeen rechtskader niet uitsluit dat er aanvullende voorschriften voor gegevensbescherming voor de politie en het gerechtelijk apparaat worden aangenomen. Voor die aanvullende voorschriften zou kunnen worden ingespeeld op de specifieke behoeften van de rechtshandhaving, vermeld in Verklaring nr. 21, die is gehecht aan het Verdrag van Lissabon ([23]).

V.2. **Herbepaling van de beginselen van gegevensbescherming**

38. In de mededeling wordt opgemerkt dat de communicatie tussen individuen en publieke en particuliere organisaties door de technologische veranderingen een transformatie ondergaat. Daarom moet volgens de Commissie een aantal basisprincipes van de gegevensbescherming opnieuw worden geformuleerd.

([19]) COM(2007) 87 def. van 7 maart 2007.

([20]) Advies van 25 juli 2007, PB C 255 van 27.10.2007, blz. 1, met name punt 30.

([21]) 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.

([22]) Arrest van het Hof van 10 februari 2009, Ierland tegen Europees Parlement en Raad van de Europese Unie in zaak C-301/96, nog niet bekendgemaakt in de Jurispr.

([23]) Zie Verklaring nr. 21 betreffende de bescherming van persoonsgegevens op het gebied van justitiële samenwerking in strafzaken en op het gebied van politiële samenwerking, gehecht aan de slotakte van de Intergouvernementele Conferentie die het Verdrag van Lissabon heeft aangenomen, PB C 115 van 9.5.2008, blz. 345.

39. De EDPS begroet die intenties van de Commissie met instemming. Het is uitermate nuttig die beginselen te beoordelen op hun doeltreffendheid met het oog op de technologische veranderingen. Ten eerste moet worden opgemerkt dat het herbepalen en herformuleren van de beginselen van gegevensbescherming niet noodzakelijk altijd verband houdt met technologische ontwikkelingen. Het kan ook vereist zijn in het perspectief van andere, in deel III hierboven genoemde ontwikkelingen: de internationalisering, het toenemende gebruik van persoonsgegevens voor de rechtshandhaving en het vrije verkeer.

40. Voorts kan die evaluatie naar het oordeel van de EDPS worden ingepast in de openbare raadpleging die door de Commissie in de Conferentie „Personal data — more use, more protection?" van 19 en 20 mei 2009 is aangekondigd. Die openbare raadpleging zou waardevolle input kunnen opleveren ([24]). De EDPS geeft in overweging dat de Raad in de tekst van het programma van Stockholm en de Commissie in haar publieke verklaringen over de openbare raadpleging inzake de toekomst van de gegevensbescherming het verband tussen de voornemens in punt 2.3 van de mededeling en de raadpleging duidelijk aangeven.

41. Ter illustratie van hetgeen onder een dergelijke evaluatie kan vallen, worden de volgende punten genoemd:

— Persoonsgegevens op het gebied van vrijheid, veiligheid en recht zijn vermoedelijk van bijzonder gevoelige aard, zoals gegevens over strafrechtelijke veroordelingen, politiële gegevens en biometrische gegevens als vingerafdrukken en DNA-profielen.

— Het verwerken daarvan kan negatieve gevolgen hebben voor de betrokkene, met name in het licht van de bevoegdheden van de rechtshandhavingsinstanties op het gebied van dwangmaatregelen. Voorts is de gegevensmonitoring en -analyse in toenemende mate geautomatiseerd, dikwijls zonder dat een mens eraan te pas komt. De technologie maakt het mogelijk gegevensbestanden met persoonsgegevens te gebruiken voor algemene zoekacties (datamining, profilering, enz.). Wettelijke verplichtingen die op gegevensverwerking rusten, dienen duidelijk vastgelegd te zijn.

— Een hoeksteen van het recht inzake gegevensbescherming is dat persoonsgegevens voor specifieke doeleinden moeten worden verzameld en niet mogen worden gebruikt op een wijze die niet verenigbaar is met die doeleinden. Gebruik voor onverenigbare doeleinden moet alleen zijn toegestaan voor zover het bij wet is vastgelegd en noodzakelijk is voor het behartigen van bepaalde publieke belangen, bijvoorbeeld de belangen die zijn vastgelegd in artikel 8, lid 2, EVRM.

— De noodzaak van inachtneming van het doelbindingsbeginsel kan gevolgen hebben voor actuele tendensen in het gegevensgebruik. Voor de rechtshandhaving worden er gegevens gebruikt die door particuliere ondernemingen voor commerciële doeleinden zijn verzameld, bijvoorbeeld in de telecommunicatie-, de transport- en de financiële sector. Daarnaast worden er grootschalige informatiesystemen opgezet, bijvoorbeeld op het gebied van immigratie en grenscontrole. Bovendien wordt er toestemming voor onderlinge schakelingen en toegang verleend, hetgeen leidt tot een verruiming van de doeleinden waarvoor de persoonsgegevens oorspronkelijk werden verzameld. Wij moeten ons bezinnen over die actuele tendensen en in het verlengde daarvan ook over eventuele aanpassingen en/of aanvullende waarborgen, waar dat noodzakelijk is.

— Behalve aan de in de mededeling vermelde beginselen van gegevensbescherming moet in het kader van de evaluatie aandacht worden geschonken aan de eis van transparantie van de verwerking, zodat het datasubject zijn rechten kan uitoefenen. Transparantie is bij uitstek een heet hangijzer in de context van de rechtshandhaving, met name omdat transparantie moet worden afgewogen tegen risico's voor het onderzoek.

— Er moeten oplossingen worden gevonden voor de uitwisselingen met derde landen.

42. De evaluatie dient zich voorts te richten op de mogelijkheden om de toepassing van de beginselen inzake gegevensbescherming doeltreffender te maken. In dat verband kan het nuttig zijn de gedachten te bepalen op instrumenten die de verantwoordelijken voor de verwerking van gegevens met sterkere verantwoordelijkheden uitrusten. Die instrumenten moeten ervoor zorgen dat de verantwoordelijken voor de verwerking van gegevens volledige verantwoording kunnen afleggen over het gegevensbeheer. „Data governance" (gegevenskwaliteitsbeheer) is een nuttig begrip in deze context. Daaronder vallen alle juridische, technische en organisatorische middelen waarmee organisaties hun volledige verantwoordelijkheid uitoefenen over de manier waarop gegevens worden behandeld, zoals planning en toezicht, gebruik van deugdelijke technologie, adequate opleiding van personeel, nalevingscontroles, enz.

V.3. **Privacyvriendelijke technologie**

43. Het verheugt de EDPS dat in punt 2.3 van de mededeling gewag wordt gemaakt van een privacycertificaat. Daaraan zouden kunnen worden toegevoegd: „privacy by design" en de noodzaak om „beste beschikbare technieken" conform het EU-gegevensbeschermingskader te bepalen.

44. Naar de mening van de EDPS kunnen „privacy by design" en privacyvriendelijke technologieën nuttige instrumenten zijn voor een betere bescherming en een doeltreffender gebruik van informatie. De EDPS stelt twee mogelijke oplossingen voor, die elkaar niet uitsluiten:

— Een privacy- en gegevensbeschermingscertificaat ([25]) als mogelijkheid voor ontwerpers en gebruikers van informatiesystemen, met of zonder EU-steun in de vorm van financiering of wetgeving.

([24]) De Groep gegevensbescherming artikel 29, waaraan de EDPS deelneemt, heeft besloten intensief te werken aan haar bijdrage aan die openbare raadpleging.

([25]) Een voorbeeld van een dergelijk certificaat is het Europees privacyzegel (European Privacy Seal, EuroPriSe).

— Een wettelijke verplichting voor ontwerpers en gebruikers van informatiesystemen om systemen te gebruiken die stroken met het beginsel van privacy by design. Hiervoor moet wellicht het toepassingsgebied van het gegevensbeschermingsrecht worden verruimd om de ontwerpers verantwoordelijk te maken voor de informatiesystemen die zij ontwikkelen ([26]).

De EDPS stelt voor om die mogelijke oplossingen in het programma van Stockholm te vermelden.

V.4. **Externe aspecten**

45. Een ander onderwerp dat in de mededeling aan de orde komt, is de ontwikkeling en de bevordering van internationale normen voor gegevensbescherming. Er worden thans tal van activiteiten ondernomen om realistische normen in te voeren die wereldwijd moeten worden toegepast, bijvoorbeeld door de International Conference of Privacy and Data Protection Commissioners. Dat zou in de nabije toekomst tot een internationale overeenkomst kunnen leiden. De EDPS geeft in overweging die activiteiten in het programma van Stockholm te ondersteunen.

46. In de mededeling wordt ook gesproken over de sluiting van bilaterale overeenkomsten op basis van reeds samen met de Verenigde Staten geboekte vooruitgang. De EDPS is het ermee eens dat er een duidelijk rechtskader moet komen voor de overdracht van gegevens aan derde landen en is derhalve verheugd over het gezamenlijke werk van de autoriteiten van de EU en de VS in de Contactgroep op hoog niveau aan een mogelijk trans-Atlantisch instrument inzake gegevensbescherming, maar pleit tegelijkertijd voor meer duidelijkheid omtrent en aandacht voor bepaalde specifieke punten ([27]). In dat perspectief is het ook interessant om nota te nemen van de ideeën in het Rapport binnenlandsezakenbeleid over een Euro-Atlantische samenwerkingsruimte van vrijheid, veiligheid en recht, waarover de EU volgens dat rapport uiterlijk in 2014 een besluit dient te nemen. Een dergelijke ruimte zou niet mogelijk zijn zonder deugdelijke waarborgen inzake gegevensbescherming.

47. Volgens de EDPS moeten de Europese normen inzake bescherming van persoonsgegevens op basis van Verdrag nr. 108 van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens ([28]) alsmede de jurisprudentie van het Europees Hof van Justitie en het Europees Hof voor de Rechten van de Mens bepalend zijn voor het beschermingsniveau in een algemene overeenkomst met de Verenigde Staten betreffende de bescherming en uitwisseling van persoonsgegevens. Een dergelijke algemene overeenkomst zou als basis kunnen dienen voor een specifieke regeling voor het uitwisselen van persoonsgegevens. Dat is des te belangrijker in het licht van het in punt 4.2.1 van de mededeling geformuleerde voornemen dat de Europese Unie waar nodig akkoorden over politiesamenwerking dient te sluiten.

48. De EDPS beseft ten volle dat de internationale samenwerking moet worden opgevoerd, in sommige gevallen ook met landen die de grondrechten niet beschermen. Het is echter ([29]) essentieel om te bedenken dat door die internationale samenwerking de verzameling en de internationale overdracht van gegevens waarschijnlijk een sterke groei zullen doormaken. Het is derhalve van wezenlijk belang dat voor de verzameling en overdracht van persoonsgegevens over de grenzen van de Unie heen de beginselen van de eerlijke en wettige verwerking — en de beginselen van de eerlijke rechtsbedeling in het algemeen — gelden, en dat persoonsgegevens slechts aan derde landen of internationale organisaties worden doorgegeven indien de betrokken derde partijen garant staan voor een toereikend beschermingsniveau of andere passende waarborgen.

49. Bij wijze van conclusie beveelt de EDPS aan om in het programma van Stockholm het belang te benadrukken van algemene overeenkomsten met de Verenigde Staten en andere derde landen inzake bescherming en uitwisseling van persoonsgegevens en dat het op het EU-grondgebied gegarandeerde beschermingsniveau daarvoor als uitgangspunt dient. Meer in het algemeen onderstreept de EDPS hoe belangrijk het is om in de betrekkingen met derde landen en internationale organisaties actief de eerbiediging van de grondrechten en met name van gegevensbescherming te bevorderen ([30]). Daarnaast zou in het programma van Stockholm het algemene principe kunnen worden opgenomen dat uitwisseling van persoonsgegevens met derde landen een adequaat beschermingsniveau of andere passende waarborgen in die derde landen vereist.

VI. **HET GEBRUIK VAN INFORMATIE**

VI.1. **Naar een Europees informatiemodel**

50. Een betere uitwisseling van informatie is voor de Europese Unie een essentieel beleidsdoel in de ruimte van vrijheid, veiligheid en recht. In punt 4.1.2 van de mededeling wordt gesteld dat de veiligheid in de Europese Unie mede wordt bepaald door de doeltreffendheid van de systemen voor de uitwisseling van informatie tussen de nationale autoriteiten en andere Europese actoren. Die benadrukking van informatie-uitwisseling ligt voor de hand gezien het ontbreken van een Europese politiedienst, een Europees strafrechtstelsel en een Europese grenscontrole. Maatregelen inzake

([26]) Gebruikers van informatie vallen onder het gegevensbeschermingsrecht, als verantwoordelijken voor de verwerking van gegevens of als verwerkers.

([27]) Zie het advies van de EDPS van 11 november 2008 over het eindverslag van de EU-VS-Contactgroep op hoog niveau inzake informatie-uitwisseling en privacy en bescherming van persoonsgegevens, PB C 128 van 6.6.2009, blz. 1.

([28]) ETS nr. 108 van 28.1.1981.

([29]) Zie de brief van de EDPS van 28 november 2005 over de mededeling van de Commissie over de externe dimensie van de ruimte van vrijheid, veiligheid en recht, beschikbaar op de website van de EDPS.

([30]) De recente vaste rechtspraak omtrent terroristenlijsten bevestigt dat er — mede in de betrekkingen met de Verenigde Staten — waarborgen vereist zijn om te garanderen dat terrorismebestrijdingsmaatregelen voldoen aan EU-normen inzake grondrechten (gevoegde zaken C-402/05 P en C-415/05 P, Kadi en Al Barakaat Foundation tegen Raad, arrest van 3 september 2008, nog niet bekendgemaakt in de Jurispr.).

informatie zijn daarom essentiële bijdragen van de Europese Unie met behulp waarvan de autoriteiten van de lidstaten doeltreffend grensoverschrijdende criminaliteit kunnen bestrijden en de externe grenzen kunnen beschermen. Zij dragen echter niet alleen bij tot de veiligheid van de burgers maar ook tot hun vrijheid — het vrije verkeer van personen werd eerder als perspectief van dit advies genoemd — en tot het recht.

51. Juist om die reden werd in het Haags Programma het beschikbaarheidsbeginsel opgenomen. Het houdt in dat voor de misdaadbestrijding vereiste informatie onbelemmerd de binnengrenzen van de EU moet kunnen passeren. Recente ervaringen wijzen uit dat het moeilijk is dat beginsel in wetgevingsmaatregelen om te zetten. Het Commissievoorstel voor een kaderbesluit van de Raad betreffende de uitwisseling van informatie volgens het beschikbaarheidsbeginsel van 12 oktober 2005 ([31]) kon niet op instemming van de Raad rekenen. De lidstaten waren niet bereid om de uiterste consequenties van het beschikbaarheidsbeginsel te aanvaarden. In plaats daarvan werden er beperktere instrumenten ([32]) aangenomen zoals Besluit 2008/615/JBZ van de Raad van 23 juni 2008 inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit („Prüm-besluit") ([33]).

52. Waar het beschikbaarheidsbeginsel nog het hart van het Haags Programma vormde, lijkt de Commissie nu een bescheidener aanpak te volgen. Zij wenst de uitwisseling van informatie tussen autoriteiten van de lidstaten verder te bevorderen door het Europees informatiemodel in te voeren. Het Zweedse EU-voorzitterschap denkt in dezelfde richting ([34]). Het zal met een voorstel voor een strategie inzake informatie-uitwisseling komen. De Raad is reeds begonnen met besprekingen over dit ambitieuze project van een informatiebeheersstrategie van de Europese Unie, die nauw verbonden is met het Europees informatiemodel. De EDPS neemt met grote belangstelling kennis van deze ontwikkelingen en wijst erop dat de aandacht in deze projecten naar gegevensbeschermingsaspecten dient uit te gaan.

Een Europees informatiemodel en gegevensbescherming

53. Om te beginnen moet worden beklemtoond dat de toekomst van de ruimte van vrijheid, veiligheid en recht niet door technologie mag worden bepaald in de zin dat de bijna grenzeloze kansen die door nieuwe technologieën worden geboden altijd moeten worden getoetst aan de desbetreffende beginselen inzake gegevensbescherming en alleen mogen worden benut indien zij aan die beginselen beantwoorden.

54. De EDPS merkt op dat het informatiemodel in de mededeling niet alleen als technisch model wordt gepresenteerd: een grotere strategische analysecapaciteit en een betere inzameling en de verwerking van operationele informatie. Ook wordt erin erkend dat er rekening moet worden gehouden met beleidsaspecten als criteria voor het inzamelen, delen en verwerken van inlichtingen, met inachtneming van de beginselen inzake gegevensbescherming.

55. Informatietechnologie en wettelijke voorwaarden zijn en blijven beide essentieel. De EDPS is ingenomen met het feit dat in de mededeling ervan wordt uitgegaan dat een Europees informatiemodel niet op technologische overwegingen mag stoelen. Het is essentieel dat informatie uitsluitend op basis van concrete veiligheidsvereisten en met inachtneming van de beginselen inzake gegevensbescherming wordt verzameld, uitgewisseld en verwerkt. De EDPS is het er ook volledig mee eens dat er een follow-upsysteem moet worden vastgesteld om het functioneren van de informatie-uitwisseling te beoordelen. Hij geeft de Raad in overweging die elementen verder uit te werken in het programma van Stockholm.

56. In dat verband onderstreept de EDPS dat gegevensbescherming ten doel heeft de burger te beschermen en niet moet worden beschouwd als iets dat een doeltreffend beheer van gegevens belemmert. Zij verschaft voorname instrumenten ter verbetering van de opslag van, de toegang tot en de uitwisseling van informatie. De rechten van het datasubject om te worden geïnformeerd over de vraag welke hem of haar betreffende informatie er wordt verwerkt en om onjuiste informatie recht te zetten, kunnen ook leiden tot een grotere precisie van de gegevens in gegevensbeheersystemen.

57. Het recht inzake gegevensbescherming komt in grote lijnen neer op het volgende: indien gegevens nodig zijn voor een specifiek en rechtmatig doel, kunnen zij worden gebruikt; zijn zij niet nodig voor een duidelijk omschreven doel, dan mogen zij niet worden gebruikt. In het eerste geval kunnen er zeer wel aanvullende maatregelen worden genomen om in adequate waarborgen te voorzien.

58. De EDPS is echter kritisch over het feit dat in de mededeling gewag wordt gemaakt van „het vaststellen van toekomstige behoeften" in de context van het informatiemodel. Hij benadrukt dat ook in de toekomst het doelbindingsbeginsel de leidraad moet zijn bij het ontwerpen van informatiesystemen ([35]). Dat is een van de essentiële waarborgen die het gegevensbeschermingssysteem de burger biedt: die moet in staat zijn van tevoren te weten voor welk doel er hem betreffende gegevens worden verzameld en dat die alleen voor dat doel worden gebruikt, met name in de toekomst. Die waarborg is zelfs verankerd in artikel 8 van het Handvest van de grondrechten van de Europese Unie. Het doelbindingsbeginsel staat uitzonderingen toe — die met name relevant zijn in de ruimte van vrijheid, veiligheid en recht — maar die uitzonderingen mogen niet bepalend zijn voor de wijze waarop het systeem wordt aangelegd.

([31]) COM(2005) 490 def.

([32]) Het Prümbesluit bevat, wat de beschikbaarheid betreft, verreikende bepalingen inzake het gebruik van biometrische gegevens (DNA en vingerafdrukken).

([33]) PB L 210 van 6.8.2008, blz. 1.

([34]) Zie het in voetnoot 5 geciteerde EU-werkprogramma van de regering, blz. 23.

([35]) Zie ook punt 41.

De juiste architectuur kiezen

59. Het begint allemaal met de keuze van de juiste architectuur voor informatie-uitwisseling. Het belang van echte architecturen van informatiesystemen wordt in de mededeling (in punt 4.1.3) onderkend, maar helaas alleen met betrekking tot interoperabiliteit.

60. De EDPS wijst daarnaast op het volgende: in het Europese informatiemodel moeten gegevensbeschermingsvereisten onlosmakelijk deel uitmaken van iedere vorm van systeemontwikkeling en niet slechts worden beschouwd als een noodzakelijke voorwaarde voor de wettelijkheid van het systeem ([36]). Er moet gebruik worden gemaakt van het begrip „privacy by design" en er moeten „beste beschikbare technieken" ([37]) worden vastgesteld (zie punt 43). Het Europees informatiemodel moet op die twee concepten worden opgebouwd. Dat houdt meer concreet in dat informatiesystemen die ten behoeve van de openbare veiligheid worden ontworpen, steevast volgens het beginsel van „privacy by design" moeten worden aangelegd. De EDPS beveelt de Raad aan om die elementen in het programma van Stockholm op te nemen.

Interoperabiliteit van systemen

61. De EDPS onderstreept dat interoperabiliteit niet een zuiver technische aangelegenheid is, maar ook implicaties heeft voor de bescherming van de burger, met name van persoonsgegevens. Vanuit het gezichtspunt van gegevensbescherming biedt een goede interoperabiliteit van systemen duidelijke voordelen aangezien dubbele opslag erdoor vermeden wordt. Het ligt echter evenzeer voor de hand dat wanneer toegang tot of uitwisseling van gegevens technisch mogelijk wordt gemaakt, dit in vele gevallen een sterke drijfveer wordt om ook daadwerkelijk toegang tot die gegevens te zoeken of ze uit te wisselen. Met andere woorden, interoperabiliteit houdt bijzondere risico's in wat betreft de onderlinge schakeling van gegevensbestanden met uiteenlopende doeleinden ([38]). De strenge beperkingen in verband met het doel van gegevensbestanden kunnen erdoor worden aangetast.

62. Kortom, het loutere feit dat het technisch mogelijk is digitale informatie uit te wisselen tussen interoperabele gegevensbanken of die gegevensbanken samen te voegen, rechtvaardigt niet dat er een uitzondering wordt gemaakt op het doelbindingsbeginsel. Interoperabiliteit moet in concrete gevallen op duidelijke en zorgvuldige beleidskeuzes gebaseerd zijn. De EDPS stelt voor dit beginsel te specificeren in het programma van Stockholm.

VI.2. **Gebruik van voor andere doeleinden verzamelde informatie**

63. Een van de belangrijkste tendensen van de afgelopen jaren, namelijk het gebruik voor wetshandhavingsdoeleinden van gegevens die in de particuliere sector voor commerciële doeleinden zijn verzameld, komt in de mededeling niet uitdrukkelijk aan bod. Deze tendens heeft niet alleen betrekking op verkeersgegevens van elektronische communicatie en passagiersgegevens van personen die naar (bepaalde) derde landen vliegen ([39]), maar geldt ook voor de financiële sector. Richtlijn 2005/60/EG van het Europees Parlement en de Raad van 26 oktober 2005 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme ([40]), is daarvan een voorbeeld. Een ander bekend en veelbesproken voorbeeld betreft de verwerking van persoonsgegevens door de Society for Worldwide Interbank Financial Telecommunication (SWIFT) ([41]), die gegevens verwerkt voor het Programma voor het traceren van terrorismefinanciering van het Amerikaanse ministerie van Financiën.

64. De EDPS is van oordeel dat deze tendensen specifieke aandacht moeten krijgen in het programma van Stockholm. Zij kunnen beschouwd worden als afwijkingen van het doelbindingsbeginsel en grijpen vaak diep in in de persoonlijke levenssfeer, omdat het gebruik van deze gegevens veel kan onthullen over het gedrag van betrokkenen. Telkens wanneer dit soort maatregelen wordt voorgesteld, moeten er zeer sterke aanwijzingen zijn dat een dergelijke ingrijpende maatregel nodig is. Zijn die aanwijzingen voorhanden, dan moet ervoor worden gezorgd dat de rechten van betrokkenen volledig gewaarborgd zijn.

65. Volgens de EDPS mogen voor commerciële doeleinden verzamelde persoonsgegevens alleen voor wetshandhaving worden gebruikt onder strikte voorwaarden, bijvoorbeeld:

— per geval moet zijn bepaald dat de gegevens uitsluitend voor specifiek omschreven doelstellingen zoals terrorismebestrijding of zware criminaliteit worden gebruikt;

— de gegevens moeten worden doorgeven via een verzoeksysteem en niet via zelfbediening ([42]);

([36]) Zie de „Guidelines and criteria for the development, implementation and use of Privacy Enhancing Security Technologies" die zijn vastgesteld in het kader van het PRISE-project (http://www.prise.oeaw.ac.at).

([37]) „Beste beschikbare technieken": het meest doeltreffende en geavanceerde ontwikkelingsstadium van de activiteiten en exploitatiemethoden, waarbij de praktische bruikbaarheid van speciale technieken is aangetoond om in beginsel de basis te vormen op grond waarvan ITS-toepassingen en -systemen aan de privacy-, gegevensbeschermings- en veiligheidsvereisten van het EU-regelgevingskader voldoen.

([38]) Zie de opmerkingen van de EDPS over de mededeling van de Commissie over de interoperabiliteit van Europese gegevensbanken van 10 maart 2006 beschikbaar op http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

([39]) Zie punt 15 hierboven.

([40]) PB L 309 van 25.11.2005, blz. 15.

([41]) Zie advies 10/2006 van 22 november 2006 over de verwerking van persoonsgegevens door de Society for Worldwide Interbank Financial Telecommunication (SWIFT) van de Werkgroep van artikel 29.

([42]) Onder „verzoeksysteem" wordt verstaan dat de verantwoordelijke voor de verwerking de gegevens op verzoek aan de wetshandhavingsdienst doorgeeft. Onder „zelfbediening" wordt verstaan dat de wetshandhavingsdienst toegang heeft tot de gegevensbank van de verantwoordelijke voor de verwerking, en de informatie uit die gegevensbank haalt. Bij het systeem van zelfbediening is het voor de verantwoordelijke voor de verwerking moeilijker om zijn verantwoordelijkheid op te nemen.

— het verzoek om gegevens moet proportioneel, nauw gespecificeerd en in beginsel gebaseerd zijn op vermoedens ten aanzien van bepaalde personen;

— routinebevragingen, datamining en het maken van profielen moeten worden vermeden;

— elk gebruik van gegevens voor wetshandhavingsdoelstellingen moet worden geregistreerd, zodat de betrokkene die zijn rechten uitoefent, de gegevensbeschermingsautoriteit en het gerechtelijk apparaat het gebruik daadwerkelijk kunnen controleren.

VI.3. **Informatiesystemen en EU-organen**

Informatiesystemen met of zonder centrale opslag ([43])

66. In de ruimte van vrijheid, veiligheid en recht is het aantal op EU-wetgeving gebaseerde informatiesystemen de afgelopen jaren beduidend toegenomen. Soms wordt besloten tot het opzetten van een systeem met centrale gegevensopslag op Europees niveau; in andere gevallen laat de wet alleen informatie-uitwisseling tussen nationale gegevensbanken toe. Het Schengeninformatiesysteem is wellicht het beste voorbeeld van een systeem met centrale opslag. Besluit 2008/615/JBZ van de Raad (het Prüm-besluit) ([44]) is vanuit het oogpunt van gegevensbescherming het meest duidelijke voorbeeld van een systeem zonder centrale opslag, aangezien het voorziet in de massale uitwisseling van biometrische gegevens tussen de autoriteiten van de lidstaten.

67. In de mededeling wordt aangetoond dat deze tendens om nieuwe systemen op te zetten zich zal doorzetten. Een eerste voorbeeld komt uit punt 4.2.2, en betreft een informatiesysteem om het Europees Strafregisterinformatiesysteem (ECRIS) uit te breiden zodat het ook onderdanen van niet-EU-landen bestrijkt. De Commissie heeft reeds opdracht gegeven voor een studie over de lijst van in de Europese Unie veroordeelde onderdanen van derde landen (EICTCN), die wellicht in een centrale gegevensbank zal resulteren. Een tweede voorbeeld, zonder centrale opslag, is de uitwisseling van informatie in het kader van e-Justice over personen die zijn vermeld in insolventieregisters in andere lidstaten (punt 3.4.1 van de mededeling).

68. Vanuit het oogpunt van gegevensbescherming zou een decentraal systeem bepaalde voordelen hebben. Dubbele gegevensopslag, met name door de autoriteiten van de lidstaat en door het centrale systeem, wordt vermeden, het is duidelijk wie verantwoordelijk is voor de gegevens aangezien de autoriteit van de lidstaat de verantwoordelijke voor de verwerking zal zijn, en de controle door de rechterlijke macht en de gegevensbeschermingsautoriteiten kan op het niveau van de lidstaten worden uitgevoerd. Maar dit systeem heeft ook zwakke punten wanneer gegevens met andere rechtsgebieden worden uitgewisseld; op dat moment moet bijvoorbeeld worden gewaarborgd dat de informatie actueel blijft in zowel het land van oorsprong als dat van bestemming, en moet aan beide kanten voor een daadwerkelijke controle worden gezorgd. Het waarborgen van de verantwoordelijkheid voor het technische systeem van de informatie-uitwisseling is zelfs nog complexer. Die zwakke punten kunnen worden opgevangen door te kiezen voor een centraal systeem, waarbij Europese instanties ten minste verantwoordelijk zijn voor onderdelen van het systeem (zoals de technische infrastructuur).

69. In dat verband zou het zinvol zijn inhoudelijke criteria op te stellen voor de keuze tussen centrale en decentrale systemen, zodat in concrete gevallen zorgvuldige beleidskeuzes kunnen worden gemaakt. Die criteria kunnen bijdragen aan de werking van de systemen zelf, maar ook aan de bescherming van de gegevens van de burgers. De EDPS stelt voor om in het programma van Stockholm het voornemen op te nemen om dergelijke criteria te ontwikkelen.

Grootschalige informatiesystemen

70. In punt 4.2.3.2 van de mededeling wordt kort stilgestaan bij de toekomst van grootschalige informatiesystemen, met een accent op het Schengeninformatiesysteem (SIS) en het visuminformatiesysteem (VIS).

71. Ook de totstandbrenging van een elektronisch systeem voor binnenkomst op en vertrek van het grondgebied van de lidstaten, alsmede programma's voor geregistreerde reizigers komen in punt 4.2.3.2 aan bod. De Commissie had dit systeem al aangekondigd als onderdeel van het pakket grensmaatregelen op initiatief van vice-voorzitter Frattini ([45]). In zijn voorlopig commentaar ([46]) is de EDPS vrij kritisch geweest over dit voorstel, omdat de noodzaak van een dergelijk ingrijpend systeem, bovenop de bestaande grootschalige systemen, onvoldoende was aangetoond. De EDPS ziet geen verdere aanwijzingen voor de noodzaak van een dergelijk systeem en stelt de Raad daarom voor dit idee niet in het programma van Stockholm op te nemen.

72. De EDPS wijst in dit verband op zijn adviezen over diverse initiatieven op het gebied van informatie-uitwisseling in de EU ([47]), waarin hij talloze suggesties heeft gedaan en is ingegaan op de gevolgen voor de gegevensbescherming van het gebruik van de grootschalige gegevensbanken op EU-niveau. Hij heeft onder meer bijzondere aandacht besteed aan de noodzaak van solide en op maat gemaakte waarborgen, alsmede aan de proportionaliteit en de

([43]) Onder centrale opslag wordt in dit verband verstaan de opslag op een centraal Europees niveau; onder decentrale opslag wordt verstaan de opslag op het niveau van de lidstaten.

([44]) Zie voetnoot 33.

([45]) Mededeling van de Commissie „De voorbereiding van de volgende stappen in het grensbeheer in de Europese Unie" — COM(2008) 69, 13.2.2008.

([46]) Voorlopig commentaar van de EDPS op drie mededelingen van de Commissie over grensbeheer (COM(2008) 69, COM(2008) 68 en COM(2008) 67) van 3 maart 2008: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

([47]) Met name: het advies van 23 maart 2005 inzake het 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, PB C 181 van 23.7.2005, blz. 13, en het advies van 19 oktober 2005 over drie voorstellen betreffende het Schengeninformatiesysteem van de tweede generatie (SIS II), PB C 91 van 19.4.2006, blz. 38.

noodzaak van effectenbeoordelingen die zijn inziens voorhanden moeten zijn voordat op dit gebied enige maatregel wordt voorgesteld of uitgevoerd. De EDPS heeft altijd gepleit voor een evenwicht tussen veiligheidsvoorschriften en de bescherming van de persoonlijke levenssfeer; een evenwicht dat correct moet zijn en aan de gegevensbeschermingsvoorschriften moet voldoen. Hij heeft hetzelfde standpunt ingenomen als toezichthouder van de centrale delen van de systemen.

73. Voorts neemt de EDPS deze gelegenheid te baat om erop te wijzen dat de informatie-uitwisseling door de EU in het algemeen een consistente aanpak behoeft en dat op het gebied van wetgeving, techniek en toezicht de bestaande systemen consistent moeten zijn met de systemen die in ontwikkeling zijn. Er is thans immers meer dan ooit een duidelijke behoefte aan een moedige en alomvattende visie over hoe de informatie-uitwisseling van de EU en de toekomstige grootschalige informatiesystemen er zouden moeten uitzien. Alleen op basis van een dergelijke visie kan een elektronisch systeem voor binnenkomst op en vertrek van het grondgebied van de lidstaten worden overwogen.

74. De EDPS stelt voor in het programma van Stockholm te vermelden dat het voornemen bestaat om die visie nader gestalte te geven; zijn inziens dient in dat kader te worden nagedacht over de mogelijke inwerkingtreding van het Verdrag van Lissabon en de gevolgen daarvan voor de systemen met een rechtsgrondslag in de eerste en derde pijler.

75. Tot slot maakt de mededeling gewag van de oprichting van een nieuw agentschap, dat volgens de mededeling ook bevoegd zou worden voor het elektronisch systeem voor binnenkomst en vertrek. De Commissie heeft inmiddels een voorstel voor de oprichting van dat agentschap aangenomen ([48]). De EDPS steunt het beginsel van dit voorstel, aangezien het de efficiëntie van de werking van deze systemen, en van de gegevensbescherming, kan vergroten. Hij zal ter zijner tijd een advies over dat voorstel uitbrengen.

Europol en Eurojust

76. De rol van Europol komt op verschillende plaatsen in de mededeling aan bod; als prioriteit wordt benadrukt dat Europol een centrale rol moet spelen op het gebied van coördinatie, uitwisseling van informatie en opleiding van beroepsbeoefenaren. Evenzeer wordt in punt 4.2.2 van de mededeling verwezen naar de recente wijzigingen in het juridisch kader van de samenwerking tussen Eurojust en Europol, en wordt aangekondigd dat de versterking van Eurojust wordt doorgetrokken, met name ten aanzien van onderzoek op het gebied van de grensoverschrijdende georganiseerde criminaliteit. De EDPS steunt deze doelstellingen ten volle, mits de waarborgen voor gegevensbescherming op passende wijze worden geëerbiedigd.

77. De EDPS is in dit verband verheugd over de recente nieuwe ontwerp-overeenkomst tussen Europol en Eurojust ([49]), die ertoe strekt de wederzijdse samenwerking tussen beide instanties te verbeteren en te versterken, en die voorziet in een efficiënte onderlinge informatie-uitwisseling. Hier ligt een opdracht waarin efficiënte en effectieve gegevensbescherming een cruciale rol speelt.

VI.4. **Het gebruik van biometrische gegevens**

78. De EDPS stelt vast dat in de mededeling geen melding wordt gemaakt van het toenemend gebruik van biometrische gegevens in verschillende rechtsinstrumenten van de Europese Unie over informatie-uitwisseling, waaronder de instrumenten tot instelling van de grootschalige informatiesystemen. Dit valt te betreuren, aangezien deze aangelegenheid vanuit het oogpunt van gegevensbescherming en persoonlijke levenssfeer van bijzonder belang en zeer gevoelig is.

79. Hoewel de EDPS de algemene voordelen van het gebruik van biometrische gegevens onderkent, heeft hij steeds de nadruk gelegd op de grote gevolgen van het gebruik van die gegevens voor de rechten van personen en heeft hij steeds voorgesteld het gebruik van biometrische gegevens in ieder afzonderlijk systeem aan strikte garanties te onderwerpen. Het recente arrest van het Europees Hof voor de Rechten van de Mens in de zaak *S. en Marper tegen het Verenigd Koninkrijk* ([50]) bevat nuttige aanwijzingen in dit verband, met name wat de rechtvaardiging en de grenzen van het gebruik van biometrische gegevens betreft. Met name kan het gebruik van DNA-gegevens gevoelige informatie over personen aan het licht brengen, mede gezien de nog steeds toenemende technische mogelijkheden om informatie uit DNA te halen. Bij grootschalig gebruik van biometrische gegevens in informatiesystemen is er tevens een probleem door de onnauwkeurigheden die inherent zijn aan het verzamelen en vergelijken van biometrische gegevens. Daarom moet de EU-wetgever terughoudendheid betrachten bij het gebruik van die gegevens.

80. Een andere kwestie die de laatste jaren steeds weer terugkomt, is het gebruik van vingerafdrukken van kinderen en ouderen, omwille van de onvolkomenheden die voor die leeftijdsgroepen inherent zijn aan biometrische systemen. De EDPS heeft om een diepgaande studie naar de nauwkeurigheid van de systemen verzocht ([51]). Hij heeft voor kinderen een leeftijdsgrens van 14 jaar voorgesteld, tenzij uit die studie blijkt dat er een andere grens moet worden vastgesteld. De EDPS beveelt aan deze kwestie in het programma van Stockholm op te nemen.

([48]) Voorstel van de Commissie van 24 juni 2009 voor een verordening van het Europees Parlement en de Raad tot oprichting van een agentschap voor het operationele beheer van het Schengeninformatiesysteem (SIS II), het Visuminformatiesysteem (VIS), EURODAC en andere grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (COM(2009) 293/2).

([49]) Door de Raad goedgekeurde maar nog door beide partijen te ondertekenen ontwerp-overeenkomst. Zie het register van Raadsdocumenten:
http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf
http://register.consilium.europa.eu/pdf/en/09/st10/st10107.en09.pdf

([50]) Gevoegde verzoekschriften 30562/04 en 30566/04, S. en Marper tegen het Verenigd Koninkrijk, arrest van 4 december 2008, EHRM, nog niet gepubliceerd.

([51]) Advies van 26 maart 2008 over het voorstel voor een verordening tot wijziging van Verordening (EG) nr. 2252/2004 van de Raad betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten, PB C 200 van 6.8.2008, blz. 1.

81. Gezien het voorgaande oppert de EDPS dat het nuttig zou zijn inhoudelijke criteria op te stellen voor het gebruik van biometrische gegevens. Die criteria moeten ervoor zorgen dat de gegevens alleen worden gebruikt wanneer zulks noodzakelijk, passend en evenredig is, en wanneer de wetgever een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde heeft aangetoond. Meer bepaald mogen biometrische gegevens, en met name DNA, niet worden gebruikt indien hetzelfde effect kan worden bereikt door gebruikmaking van andere, minder gevoelige, informatie.

VII. **TOEGANG TOT JUSTITIE EN E-JUSTICE**

82. Technologie zal ook als instrument voor een betere justitiële samenwerking worden gebruikt. In punt 3.4.1 van de mededeling wordt e-Justice voorgesteld als een middel om de toegang van burgers tot de rechter te verbeteren. E-Justice bestaat uit een portaal met informatie en videoconferenties als onderdeel van de juridische procedure. Zij biedt voorts de mogelijkheid tot online juridische procedures, en de koppeling van nationale registers, zoals insolventieregisters, is ook gepland. De EDPS neemt er nota van dat in de mededeling geen nieuwe initiatieven met betrekking tot e-Justice worden vermeld, maar dat louter acties worden geconsolideerd die reeds op gang zijn gebracht. De EDPS is bij een aantal van die acties betrokken, in het kader van de follow-up van het advies dat hij op 19 december 2008 heeft uitgebracht over de Commissiemededeling „Naar een Europese strategie inzake e-Justice" ([52]).

83. E-Justice is een ambitieus project dat ten volle moet worden gesteund. Dit project kan het rechtsstelsel in Europa en de rechtsbescherming van de burger daadwerkelijk verbeteren. Het is een belangrijke stap op weg naar een Europese rechtsruimte. Deze positieve beoordeling voor ogen houdend, kan toch een aantal opmerkingen worden gemaakt:

— De technologische systemen voor e-Justice moeten worden ontworpen volgens het beginsel inzake „privacy by design". Zoals eerder gezegd, begint — wat het Europese informatiemodel betreft — alles bij de keuze van de juiste architectuur.

— Bij de koppeling en de interoperabiliteit van systemen moet het doelbindingsbeginsel worden geëerbiedigd.

— De verantwoordelijkheden van de verschillende actoren moeten precies worden omschreven.

— De gevolgen die de koppeling van nationale registers met delicate persoonsgegevens, zoals insolventieregisters, voor personen heeft, moeten van tevoren worden onderzocht.

VIII. **CONCLUSIES**

84. De EDPS onderschrijft de nadruk die in de mededeling wordt gelegd op de bescherming van de grondrechten, en in het bijzonder op de bescherming van persoonsgegevens, die een van de belangrijkste vraagstukken voor de toekomst van de ruimte van vrijheid, veiligheid en recht vormt. Volgens de EDPS wordt in de mededeling terecht gepleit voor een evenwicht tussen de behoefte aan passende instrumenten om de veiligheid van de burgers te waarborgen en de bescherming van hun grondrechten. Tevens wordt in de mededeling onderkend dat meer nadruk moet worden gelegd op de bescherming van persoonsgegevens.

85. De EDPS steunt ten volle punt 2.3 van de mededeling, waarin onafhankelijk van de inwerkingtreding van het Verdrag van Lissabon, een oproep wordt gedaan tot het invoeren van een integrale gegevensbeschermingsregeling voor alle bevoegdheidsgebieden van de EU. Hij beveelt in dit verband aan:

— in het programma van Stockholm op te nemen dat er een duidelijke langetermijnvisie voor die integrale regeling moet komen;

— de op dit gebied vastgestelde maatregelen, alsook de concrete uitvoering en de doeltreffendheid ervan, te evalueren, rekening houdend met de gevolgen voor de persoonlijke levenssfeer en met de doeltreffendheid van de wetshandhaving;

— in het programma van Stockholm als prioriteit op te nemen dat er een nieuw wetgevingskader moet komen, waarbij onder meer Kaderbesluit 2008/977/JBZ van de Raad wordt vervangen.

86. De EDPS is ingenomen met het voornemen van de Commissie om opnieuw de beginselen inzake gegevensbescherming te bevestigen, die in verband moeten worden gebracht met de openbare raadpleging die door de Commissie in de conferentie „Personal data — more use, more protection?" van 19 en 20 mei 2009 is aangekondigd. Wat de inhoud betreft, beklemtoont de EDPS het belang van het doelbindingsbeginsel als hoeksteen van de wetgeving inzake gegevensbescherming, en onderstreept hij dat men zich moet richten op de mogelijkheden om de toepassing van de beginselen inzake gegevensbescherming doeltreffender te maken, zulks met instrumenten die de verantwoordelijkheden van de verantwoordelijken voor de verwerking van gegevens kunnen versterken.

87. „Privacy by design" en privacyvriendelijke technologieën kunnen worden gestimuleerd door:

— een privacy- en gegevensbeschermingscertificaat als optie voor ontwerpers en gebruikers van informatiesystemen;

— een wettelijke verplichting voor ontwerpers en gebruikers van informatiesystemen om systemen te gebruiken die stroken met het beginsel inzake privacy by design.

88. Wat de externe aspecten van gegevensbescherming betreft, beveelt de EDPS aan:

— in het programma van Stockholm de nadruk te leggen op het belang van algemene overeenkomsten met de Verenigde Staten en andere derde landen over gegevensbescherming en gegevensuitwisseling;

([52]) Advies van de EDPS van 19 december 2008 over de Mededeling van de Commissie „Naar een Europese strategie inzake e-Justice", PB C 128 van 6.6.2009, blz. 13.

— de eerbiediging van de grondrechten, en met name van gegevensbescherming, actief te bevorderen in de betrekkingen met derde landen en met internationale organisaties;

— in het programma van Stockholm op te nemen dat uitwisseling van persoonsgegevens met derde landen een adequaat beschermingsniveau of andere passende waarborgen in die derde landen vereist.

89. De EDPS neemt met grote belangstelling nota van de ontwikkelingen op weg naar een informatiebeheersstrategie van de Europese Unie en een Europees informatiemodel en wijst erop dat de aandacht in deze projecten naar gegevensbeschermingsaspecten dient uit te gaan. De architectuur voor gegevensuitwisseling moet op „privacy by design" en „beste beschikbare technieken" gebaseerd zijn.

90. Het loutere feit dat het technisch mogelijk is digitale informatie uit te wisselen tussen interoperabele gegevensbanken of die gegevensbanken samen te voegen, rechtvaardigt niet dat er een uitzondering wordt gemaakt op het doelbindingsbeginsel. Interoperabiliteit moet in concrete gevallen op duidelijke en zorgvuldige beleidskeuzes gebaseerd zijn. De EDPS stelt voor dit begrip te specificeren in het programma van Stockholm.

91. Het gebruik ten behoeve van wetshandhaving van voor commerciële doeleinden verzamelde persoonsgegevens mag volgens de EDPS alleen worden toegestaan onder strikte voorwaarden, die in punt 65 van dit advies vervat zijn.

92. Andere voorstellen betreffende het gebruik van persoonsgegevens zijn onder meer:

— Het opstellen van inhoudelijke criteria voor de keuze tussen een gecentraliseerd en een gedecentraliseerd systeem, en het opnemen in het programma van Stockholm van het voornemen om dergelijke criteria te ontwikkelen.

— De totstandbrenging van een elektronisch systeem voor binnenkomst op en vertrek van het grondgebied van de lidstaten, parallel aan geregistreerde reizigersprogramma's hoeven niet in het programma van Stockholm te worden vermeld.

— Steun voor de versterking van Europol en Eurojust en voor de recente nieuwe overeenkomst tussen Europol en Eurojust.

— Het opstellen van inhoudelijke criteria voor het gebruik van biometrische gegevens, waarbij ervoor wordt gezorgd dat de gegevens alleen worden gebruikt wanneer zulks noodzakelijk, passend en evenredig is, en wanneer de wetgever een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel heeft aangetoond. DNA mag niet worden gebruikt indien hetzelfde effect kan worden bereikt door gebruikmaking van andere, minder gevoelige gegevens.

93. De EDPS steunt e-Justice en heeft een aantal opmerkingen gemaakt over hoe dit project kan worden verbeterd (zie punt 83).

Gedaan te Brussel, 10 juli 2009.

Peter HUSTINX

Europees Toezichthouder voor gegevensbescherming