EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING

Advies van de Europese Toezichthouder voor gegevensbescherming 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 (COM(2004)835 def.)

(2005/C 181/06)

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING,

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

Gelet op het Handvest van de grondrechten van de Europese Unie, 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 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 gelet op artikel 41,

Gezien de op 25 januari 2005 ontvangen adviesaanvraag van de Commissie overeenkomstig artikel 28, lid 2, van Verordening (EG) nr. 45/2001;

BRENGT HET VOLGENDE ADVIES UIT:

1. **INLEIDING**

1.1. **Opmerkingen vooraf**

Over het opzetten van het Visuminformatiesysteem (VIS), een belangrijk onderdeel van het gemeenschappelijk visumbeleid van de EU, bestaan diverse onderling verwante teksten.

— In april 2003 is in opdracht van de Commissie een haalbaarheidsstudie uitgebracht over het VIS [1].

— In september 2003 stelde de Commissie wijzigingen [2] voor op de verordening betreffende het uniforme visummodel. De voornaamste doelstelling was dat in het nieuwe model ook biometrische gegevens (gezichtsopname en twee vingerafdrukken) zouden worden opgenomen. Deze gegevens zouden worden opgeslagen in een microchip.

[1] Visa Information System, eindrapport van Trasys, in opdracht van de Commissie, april 2003.
[2] COM(2003)558 def.; interinstitutionele dossiers 2003/0217 (CNS) en 2003/0218 (CNS).

— In juni 2004 is bij besluit van de Raad ([1]) het startsein gegeven voor het opzetten van het VIS en dus ook de rechtsgrondslag gelegd voor de budgettering ervan. Volgens dit besluit komt er een centrale databank met informatie over visumaanvragen, evenals een comitologieprocedure voor het beheer van de technische ontwikkeling van het VIS.

In december 2004 heeft de Commissie een voorstel tot verordening betreffende het VIS en de uitwisseling van informatie inzake visa voor kort verblijf („het voorstel") aangenomen ([2]). Dit voorstel is het onderwerp van dit advies. Bij het voorstel is een uitgebreide effectbeoordeling ([3]) („het EIA") gevoegd.

Zoals in de toelichting staat, zal de verordening echter moeten worden aangevuld met verdere wetgeving, met name om:

— in verband met de invoering van biometrische gegevens de gemeenschappelijke instructies aan de diplomatieke en consulaire beroepsposten van de partijen bij de Schengenovereenkomst („de Gemeenschappelijke Visuminstructies") te wijzigen;

— een nieuw systeem voor de gegevensuitwisseling met Ierland en het Verenigd Koninkrijk te ontwikkelen;

— informatie over visa voor lang verblijf uit te wisselen.

Zoals de Raad Justitie en Binnenlandse Zaken van 5 en 6 juni 2003 heeft besloten en in artikel 1, lid 2, van bovengenoemd Raadsbesluit van juni 2004 beschreven staat, zal het VIS worden gebaseerd op een gecentraliseerde architectuur en bestaan uit een gegevensbank met de visumaanvragen: het centrale visuminformatiesysteem (CS-VIS) en per lidstaat een nationale interface (NI-VIS). De lidstaten wijzen ieder een centrale autoriteit ([4]) aan, die met de nationale interface is verbonden en via welke hun bevoegde autoriteiten toegang zullen hebben tot het CS-VIS.

1.2. **Hoofdpunten van het voorstel vanuit het oogpunt van gegevensbescherming**

Het voorstel is erop gericht de toepassing van het gemeenschappelijk visumbeleid te verbeteren dankzij een vlottere uitwisseling van informatie tussen de lidstaten via een centrale databank. Tijdens de aanvraagprocedure worden biometrische gegevens (foto en vingerafdrukken) ingevoerd en in de centrale gegevensbank opgeslagen.

Volgens een Commissievoorstel tot wijziging van de verordening over het uniforme model zouden biometrische gegevens ook gebruikt kunnen worden in de visumsticker, die een microchip zou bevatten waarin een foto en vingerafdrukken zijn opgeslagen (de Raad wacht hiervoor op de resultaten van een analyse).

Het voorstel bevat een gedetailleerde beschrijving van de verschillende verrichtingen (invoeren, wijzigen, verwijderen en raadplegen van gegevens) en van de verschillende gegevens die naar gelang van het resultaat van de aanvraag (inwilliging, weigering, …) moeten worden ingevoerd.

Van elke aanvraag zouden de gegevens vijf jaar moeten worden bewaard.

Er wordt een limitatieve opsomming gegeven van de andere bevoegde instanties dan de visumautoriteiten die toegang zullen hebben tot het VIS, en er wordt bepaald wat die toegang zal inhouden:

— de autoriteiten die bevoegd zijn voor visumcontrole aan de buitengrenzen en op het grondgebied van de lidstaat,

— de bevoegde immigratieautoriteiten,

([1]) 2004/512/EG, PB L 213, 15.6.2004, blz. 5.
([2]) COM(2004)835 def.; interinstitutioneel dossier 2004/0287 (COD).
([3]) Study for the Extended Impact Assessment of the Visa Information System; eindverslag van EPEC, december 2004.
([4]) Artikel 24, lid 2, van het voorstel.

— de bevoegde asielautoriteiten.

Wat het beheer en de verantwoordelijkheden betreft, staat in het voorstel dat de Commissie de VIS-gegevens namens de lidstaten zal verwerken. Ter wille van de beveiliging moeten de gegevens worden geregistreerd; de respectieve taken in verband met deze beveiliging worden uitvoerig beschreven.

Het voorstel bevat een hoofdstuk over gegevensbescherming, met een gedetailleerde omschrijving van de taken van de nationale autoriteiten en van de Europese Toezichthouder voor gegevensbescherming („de EDPS").

De technische implementatie van het VIS en de keuze van de benodigde technologie worden opgedragen aan het comité dat is ingesteld bij artikel 5, lid 1, van Verordening (EG) nr. 2424/2001 van de Raad van 6 december 2001 betreffende de ontwikkeling van een Schengeninformatiesysteem van de tweede generatie (SIS II).

Het voorstel gaat vergezeld van een uitgebreide effectbeoordeling, die in opdracht van de Commissie door EPEC is verricht. De conclusie luidt dat een VIS met biometrische gegevens de beste beschikbare optie ter verbetering van het gemeenschappelijk visumbeleid is.

2. **TOEPASSELIJK KADER**

Het voorstel zal grote implicaties hebben voor de persoonlijke levenssfeer en andere individuele grondrechten; het moet daarom worden getoetst aan de gegevensbeschermingsbeginselen. Hier volgen de voornaamste referentiepunten:

— De eerbiediging van het privéleven is in Europa gewaarborgd sinds de Raad van Europa in 1950 het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden („het EVRM") heeft aangenomen. In artikel 8 daarvan is het „recht op eerbiediging van privé, familie- en gezinsleven" neergelegd.

  Volgens artikel 8, lid 2, is „geen inmenging van enig openbaar gezag in de uitoefening van dit recht (…) toegestaan dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is" ter bescherming van zwaarwegende belangen. Deze voorwaarden hebben ertoe geleid dat het Europees Hof voor de rechten van de mens extra eisen heeft gesteld met betrekking tot de hoedanigheid van de rechtsgrond voor overheidsinmenging, de evenredigheid van een maatregel en passende waarborgen tegen misbruik.

  De basisbeginselen voor de bescherming van personen met betrekking tot de verwerking van persoonsgegevens zijn neergelegd in het in de Raad van Europa tot stand gekomen Verdrag van 1981 inzake gegevensbescherming.

— De eerbiediging van het privé-leven en van het familie- en gezinsleven, alsmede de bescherming van persoonsgegevens zijn meer recentelijk verankerd in de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, dat als deel II in de nieuwe EU-Grondwet is opgenomen.

  Krachtens artikel 52 van het Handvest kunnen deze rechten aan beperkingen worden onderworpen, op de voorwaarden die ook op grond van artikel 8 van het EVRM gelden. Bij de beoordeling van voorstellen tot mogelijke inmenging moet met die voorwaarden rekening worden gehouden.

Momenteel is de basiswetgeving van de EU over gegevensbescherming vervat in twee teksten:

— 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, blz. 31; „Richtlijn 95/46/EG"). In de richtlijn wordt uitvoerig aangegeven aan welke beginselen de voorgestelde verordening zal moeten voldoen voor zover zij op de lidstaten van toepassing is. Het belang hiervan schuilt ook in het feit dat de verordening in combinatie met de nationale uitvoeringswetgeving voor de richtlijn zal worden toegepast. In hoeverre de voorgestelde bepalingen en waarborgen doel zullen treffen, hangt dus af van de mate waarin die combinatie daar in ieder afzonderlijk geval in zal slagen.

— Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (PB L 8, blz. 1; „Verordening nr. 45/2001"). Zij bevat beginselen welke te vergelijken zijn met die van Richtlijn 95/46/EG en is hier van belang voor zover de voorgestelde verordening, samen met Verordening nr. 45/2001, van toepassing zal zijn op de werkzaamheden van de Commissie. Ook deze combinatie verdient daarom aandacht.

Richtlijn 95/46/EG en Verordening nr. 45/2001 moeten samen met andere wetteksten worden gelezen. Met andere woorden, voor zover de richtlijn en de verordening handelen over verwerking van persoonsgegevens die inbreuk kan maken op de fundamentele vrijheden, in het bijzonder het recht op eerbiediging van het privé-leven, moeten zij in het licht van de grondrechten worden uitgelegd. Dit volgt ook uit de jurisprudentie van het Hof van Justitie ([1]).

— Tot slot zal in de analyse van het voorstel ook advies nr. 7/2004 worden meegenomen, dat de „Groep gegevensbescherming van artikel 29" op 11 augustus 2004 ([2]) heeft uitgebracht „over de opneming van biometrische elementen in verblijfsvergunningen en visa in verband met de instelling van het Europese visuminformatiesysteem (VIS)", en waarin tegen diverse punten uit het voorstel bezwaren worden ingebracht. De EDPS zal nagaan of en hoe aan die bezwaren tegemoet is gekomen.

3. ANALYSE VAN HET VOORSTEL

3.1. Algemeen

De EDPS erkent dat de verdere ontwikkeling van een gemeenschappelijk visumbeleid efficiënte gegevensuitwisseling impliceert. Het VIS is een van de instrumenten die voor een vlotte informatiestroom kunnen zorgen. Zo'n nieuw instrument dient echter beperkt te blijven tot het verzamelen en uitwisselen van gegevens, voor zover dat verzamelen en uitwisselen nodig is voor, en evenredig is met de verwezenlijking een gemeenschappelijk visumbeleid.

Het VIS kan een positief effect hebben op andere rechtmatige publieke belangen, hetgeen echter niets verandert aan de opzet ervan. Die opzet is beperkt, wat van groot belang is bij het bepalen van de rechtmatigheid van inhoud en toepassing van het systeem, en dus bij het verlenen van toegang tot het VIS (of delen ervan) aan autoriteiten van de lidstaten in het rechtmatig openbaar belang.

Daarnaast zullen volgens het voorstel biometrische gegevens in het VIS worden ingevoerd. De EDPS erkent de voordelen hiervan, maar wijst op de enorme consequenties en stelt voor dat dit met stringente waarborgen wordt omgeven.

Dit advies staat in het teken van deze centrale beschouwingen. Er zij op gewezen dat het advies moet worden aangehaald in de preambule van de verordening, vóór de overwegingen („Gezien het advies ...").

([1]) Hier zij verwezen naar het arrest dat het Hof van Justitie op 20 mei 2003 in voltallige zitting heeft gewezen in de gevoegde zaken C-465/00, C-138/01 en C-139/01 (Österreichischer Rundfunk e.a., Jurispr. 2003, blz. I-4989). Het Hof moest zich uitspreken over een Oostenrijkse wet die toestond dat salarisgegevens van ambtenaren aan de Oostenrijkse Rekenkamer werden meegedeeld en vervolgens werden gepubliceerd. Uit artikel 8 van het EVRM leidde het Hof een aantal criteria af die moeten worden gehanteerd bij de toepassing van Richtlijn 95/46/EG, voor zover deze richtlijn beperkingen op het recht op eerbiediging van de privacy mogelijk maakt.

([2]) Een onafhankelijke adviesgroep, bestaande uit vertegenwoordigers van de nationale gegevensbeschermingsautoriteiten, van de EDPS en van de Commissie; de groep is ingesteld bij Richtlijn 95/46/EG.

3.2. **Doel**

Zowel in het licht van artikel 8 van het EVRM als van het algemene gegevensbesschermingsbestel is het VIS van cruciaal belang. Volgens artikel 6 van Richtlijn 95/46/EG moeten persoonsgegevens„voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden … worden verkregen en vervolgens niet worden verwerkt op een wijze die onverenigbaar is met die doeleinden". Alleen aan de hand van duidelijk omschreven doeleinden zal precies uit te maken zijn of de verwerking van persoonsgegevens evenredig en toereikend is — een criterium dat, gezien de aard van de (onder meer biometrische)gegevens en de omvang van de voorgenomen operatie, van essentieel belang is.

Het doel van het VIS staat duidelijk omschreven in artikel 1, lid 2, van het voorstel:

> „Het VIS moet het beheer van het gemeenschappelijk visumbeleid, de consulaire samenwerking en het overleg tussen de centrale autoriteiten die bevoegd zijn voor consulaire zaken verbeteren door de uitwisseling van gegevens tussen de lidstaten betreffende aanvragen en de daartoe genomen beslissingen te vergemakkelijken".

Het VIS moet dus in al zijn onderdelen een noodzakelijk en evenredig instrument zijn bij de verwezenlijking van dit beleidsdoel, ten behoeve van het gemeenschappelijk visumbeleid.

In artikel 1, lid 2, worden ook bijkomende voordelen van een beter visumbeleid opgesomd, zoals:

a) het voorkomen van bedreigingen van de interne veiligheid;

c) de vergemakkelijking van fraudebestrijding;

d) de vergemakkelijking van controles aan de buitengrenzen.

De EDPS beschouwt dit als positieve uitvloeisels van het opzetten van het VIS en van de verbetering van het gemeenschappelijk visumbeleid, maar niet als doelstellingen op zich.

Er zijn dus momenteel twee grote conclusies te trekken:

— De EDPS is zich ervan bewust dat de rechtshandhavingsinstanties er belang bij hebben toegang te krijgen tot het VIS; de Raad heeft op 7 maart 2005 conclusies in die zin aangenomen. Maar het VIS heeft tot doel heeft het gemeenschappelijk visumbeleid te verbeteren, en een routinematige toegang tot het systeem door de rechtshandhavingsinstanties is niet in overeenstemming met dit doel. Krachtens artikel 13 van Richtlijn 95/46/EC kan toegang niet stelselmatig worden verleend, maar uitsluitend op ad-hoc basis, in specifieke omstandigheden en mits passende garanties worden geboden.

  Meer in het algemeen zullen, indien ooit beslist wordt of andere autoriteiten tot het VIS moeten worden toegelaten, in ieder geval de evenredigheid en de noodzaak hiervan moeten worden aangetoond. Toegang kan alleen worden verleend voor operaties die met de doelstellingen van het VIS te verenigen zijn.

— De vermelding in a), namelijk het voorkomen van „bedreigingen van de interne veiligheid van de lidstaten", is ongelukkig. Het VIS zal vooral resultaten afwerpen op het gebied van fraudebestrijding en visumshoppen (fraudebestrijding is overigens het voornaamste motief voor de invoer van biometrische gegevens) ([1]). Het voorkomen van bedreigingen van de veiligheid moet dus worden beschouwd als een „afgeleid", zij het zeer welkom, effect.

  De EDPS beveelt aan om in artikel 1, lid 2, een explicieter onderscheid te maken tussen „doelstelling" en „positieve consequenties"; bijvoorbeeld als volgt:

  „Het VIS heeft tot doel het beheer van het gemeenschappelijk visumbeleid, de consulaire samenwerking en het overleg tussen de centrale autoriteiten die bevoegd zijn voor consulaire zaken te verbeteren door de uitwisseling van gegevens tussen de lidstaten betreffende aanvragen en de daarover genomen beslissingen te vergemakkelijken. Het draagt er zodoende tevens toe bij dat …".

([1]) In de EIA wordt dit expliciet gezegd (blz.6, §2.7): *„the inefficiencies in combating visa shopping, fraud, and in conducting checks are causing also inefficiencies in relation to internal security of the Member States"*. Dit betekent dat bedreigingen van de veiligheid deels te wijten zijn aan een ondoeltreffend visumbeleid. Het is allereerst zaak het visumbeleid te verbeteren, vooral door middel van fraudebestrijding en betere controles. Een beter visumbeleid zal meer veiligheid opleveren.

Het is trouwens opmerkelijk dat in de richtsnoeren voor de instelling van een gemeenschappelijk systeem voor de uitwisseling van informatie, die de Raad JBZ op 13 juni 2002 heeft aangenomen [1], de preventie van bedreigingen van de interne veiligheid aan het eind van de lijst staat. Dit zou ook in de hier besproken tekst mogelijk zijn, en het zou veel beter aansluiten bij de opzet van het VIS.

3.3. **Kwaliteit van de gegevens**

Volgens artikel 6 van Richtlijn 95/46/EG moeten persoonsgegevens „toereikend, terzake dienend en niet bovenmatig … zijn, uitgaande van de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt". Dit geldt voor de evenredigheid van het VIS zelf, maar ook voor de gegevens die worden ingezameld en opgeslagen, voor het verdere gebruik ervan, en voor de extra garanties die in dit verband van toepassing zijn. Deze elementen zijn gelijkelijk cruciaal bij de toetsing van het voorstel aan artikel 8 van het EVRM.

Het VIS zal ongetwijfeld fors ingrijpen in de uitoefening van het recht op eerbiediging van de persoonlijke levenssfeer, al was het maar wegens de omvang ervan en de aard van de verwerkte persoonsgegevens. Daarom heeft de Groep van artikel 29 in advies nr. 7/2004 de wens uitgesproken te vernemen welke studies naar de omvang en de ernst van de bewuste fenomenen, dwingende overwegingen van openbare veiligheid en openbare orde aan het licht hebben gebracht die een dergelijke aanpak rechtvaardigen.

De EDPS heeft zorgvuldig nota genomen van de bewijzen uit het EIA. Hoewel niet geheel sluitend, blijken zij toch voldoende materiaal op te leveren om het opzetten van een VIS ter verbetering van het gemeenschappelijk visumbeleid te rechtvaardigen.

Gegeven deze context, ligt het binnen het bereik van de wetgever om uit te maken of het VIS zal worden ingesteld als instrument om de afgifte van visa door de lidstaten beter te laten verlopen. Zo'n systeem zou op zich goed passen in de geleidelijke vorming van een ruimte van vrijheid, veiligheid en rechtvaardigheid in de zin van het EG-Verdrag, en dat proces zelfs schragen.

Niettemin kan de instelling en de toepassing van het VIS nooit tot gevolg hebben dat een hoog niveau van bescherming van persoonsgegevens op dit gebied niet te handhaven is. De adviestaak van de EDPS houdt ook in na te gaan in welke mate het VIS invloed heeft op het bestaande gegevensbeschermingsniveau voor de betrokkenen.

De EDPS zal hier daarom nader ingaan op de volgende punten:

— het evenredige en toereikende karakter van de gegevens en het gebruik ervan (bv. gegevenscategorieën, toegang tot gegevens voor de verschillende betrokken instanties, bewaringstermijn);

— het systeembeheer (bv. verantwoordelijkheden en beveiliging);

— de rechten van de betrokkenen (bv. informatie, mogelijkheid onjuiste of irrelevante gegevens recht te zetten of te verwijderen);

— toezicht en supervisie.

Afgezien van de navolgende paragrafen geeft het voorstel geen aanleiding tot belangrijke opmerkingen over de gegevenscategorieën die in het VIS zullen worden opgenomen, noch over het gebruik ervan. De desbetreffende bepalingen zijn met de nodige zorg geredigeerd en lijken al bij al consistent en adequaat.

[1] Kaderbesluit 2002/475/JBZ van de Raad van 13 juni 2002 inzake terrorismebestrijding, PB L 164 van 22.6.2002, blz. 3.

3.4. **Biometrische gegevens**

3.4.1. *Impact van het gebruik van biometrische gegevens*

De beslissing om in een informatiesysteem biometrische gegevens op te slaan kan nooit als onbelangrijk worden afgedaan, vooral niet als dat systeem zo ontzaglijk veel mensen raakt. Het betreft hier niet zomaar een nieuwe informatietechnologie. Biometrische informatie brengt onherroepelijk een verandering teweeg in de relatie tussen lichaam en identiteit, omdat de eigenschappen van het menselijk lichaam „leesbaar" worden gemaakt voor de machine, en vatbaar zijn voor verder gebruik. Ook al zijn biometrische kenmerken niet zichtbaar voor het menselijk oog, met de juiste instrumenten kunnen zij altijd en overal zichtbaar en bruikbaar worden gemaakt .

Hoe nuttig biometrica voor bepaalde doeleinden ook mogen zijn, de grootschalige toepassing ervan zal een enorme impact hebben op de samenleving en zou het voorwerp moeten uitmaken van een brede en open discussie. De EDPS moet constateren dat deze discussie niet echt heeft plaatsgevonden voordat het voorstel werd uitgewerkt. Dit maakt de behoefte aan stringente waarborgen bij het gebruik van biometrische gegevens en aan zorgvuldig beraad en overleg tijdens de wetgevingsprocedure des te prangender.

3.4.2. *Specifieke aard van biometrische gegevens*

Zoals al onderstreept werd in verscheidene adviezen van de Groep van artikel 29 ([1]), moet de invoering en verwerking van biometrische gegevens voor identiteitsdocumenten gepaard gaan met een uitermate consistente en degelijke beveiliging. Die gegevens zijn, vanwege enkele specifieke kenmerken, immers zeer gevoelig.

In tegenstelling tot een wachtwoord of een sleutel kan iemand zijn biometrische gegevens niet kwijtraken. Zij bieden een *bijna absoluut onderscheidend vermogen*: ieder individu bezit unieke biometrische kenmerken. Deze veranderen gedurende het gehele leven bijna nooit, waardoor zij een *permanent karakter* hebben. Ieder mens heeft dezelfde biometrische „elementen", waardoor deze een *universele* dimensie krijgen.

Herziening van biometrische gegevens is dus bijna onmogelijk: het is moeilijk om een vinger of een gezicht te veranderen. Dit -in vele opzichten positieve- aspect heeft, in geval van *ontvreemding van identiteit*, een groot nadeel: de in een databank opgeslagen vingerafdrukken en foto's die verband houden met een gestolen identiteitsdocument kunnen de werkelijke eigenaar van die identiteit onophoudelijk grote problemen bezorgen. Biometrische gegevens zijn per definitie *niet geheim* en kunnen *sporen achterlaten* (vingerafdruk, DNA), waardoor die gegevens verzameld kunnen worden *zonder dat de eigenaar zich daarvan bewust is*.

Vanwege deze aan biometrische gegevens inherente risico's moet er voor een goede bescherming worden gezorgd (vooral in de zin van het beginsel aangaande de beperking van het doel, de beperking van de toegang en beveiligingsmaatregelen).

3.4.3. *Technische tekortkomingen van vingerafdrukken*

De belangrijkste van de hierboven beschreven voordelen van biometrische gegevens (het universele en onderscheidende karakter, bruikbaarheid, enz.) zijn nooit absoluut. Dat heeft directe gevolgen voor de efficiëntie van de in de verordening voorgeschreven procedures voor invoering en verificatie van gegevens.

Naar schatting ([2]) kunnen de gegevens van zo'n 5 % van de mensen niet worden ingevoerd (omdat deze onleesbare of helemaal geen vingerafdrukken hebben). Het aan het voorstel gehechte EIB voorspelt voor 2007 ongeveer 20 miljoen visumaanvragen, wat betekent dat voor ongeveer 1 miljoen personen niet de „normale" invoeringsprocedure gevolgd kan worden, met evidente gevolgen voor de visumaanvraag en de grenscontroles.

([1]) Advies 7/2004 over de opneming van biometrische elementen in verblijfsvergunningen en visa, rekening houdend met de oprichting van het Europese visuminformatiesysteem (VIS) (Markt/11487/04/EN-WP 96) en het werkdocument over biometrische gegevens (MARKT/10595/03/EN-WP 80)

([2]) A. Sasse, *Cybertrust and Crime Prevention: Usability and Trust in Information Systems*, in „Foresight cybertrust and crime prevention project", 04/1151, 10 juni 2004, blz. 7, en Technology Assessment, „Using Biometrics for Border Security", United States General Accounting Office, GAO-03-174, november 2002.

Biometrische identificatie is ook per definitie een statistische aangelegenheid. Een foutenmarge van 0,5 à 1 % is normaal ([1]), wat betekent dat het controlesysteem aan de buitengrens een foutieve afwijzing (FRR) van 0,5 à 1 % zal hebben. Dat percentage is afgestemd op een drempel gebaseerd op de risico-analyse van de bevoegde autoriteiten (het komt overeen met het tegen elkaar wegstrepen van de ten onrechte afgewezen en de ten onrechte toegelaten personen). Het is daarom overdreven om te zeggen dat die technologie voor een „accurate identificatie" kan zorgen, zoals beweerd wordt in de negende overweging van het verordeningsvoorstel.

Volgens een recente prospectieve studie ([2]) die de Commissie LIBE van het Europees Parlement besteld had, moeten er *vangnetprocedures* komen voor het invoeren van biometrische gegevens, omdat deze niet voor iedereen toegankelijk en niet volledig accuraat zijn. Die procedures moeten worden toegepast en gebruikt met het oog op de waardigheid van personen van wie de gegevens niet ingevoerd konden worden, en om te vermijden dat zij het slachtoffer worden van de tekortkomingen van het systeem. ([3])

De EDPS beveelt derhalve aan vangnetprocedures te ontwikkelen en in het voorstel op te nemen. Deze procedures mogen geen afbreuk doen aan de veiligheid van het visabeleid en mensen met onleesbare vingerafdrukken niet stigmatiseren.

3.5 **Speciale gegevenscategorieën**

Bepaalde gegevenscategorieën (anders dan biometrische) vergen speciale aandacht, namelijk de redenen voor de weigering van een visum (3.5.1) en gegevens over andere leden van een groep (3.5.2).

3.5.1. *Redenen voor weigering van een visum*

Artikel 10, lid 2, van het voorstel betreft de verwerking van de gegevens die verband houden met de weigering, wanneer besloten is een visum te weigeren. De redenen voor die weigering zijn volledig gestandaardiseerd.

— de eerste twee redenen in de punten a) en b) zijn eerder van administratieve aard: het niet kunnen voorleggen van een geldig reisdocument, of het niet kunnen voorleggen van geldige documenten waaruit het doel en de voorwaarden van het voorgenomen verblijf blijken;

— punt c) luidt: „de aanvrager staat gesignaleerd met de bedoeling de toegang te weigeren"; dat impliceert raadpleging van het SIS-gegevensbestand;

— punt d) geeft als reden voor weigering van een visum het feit op dat de aanvrager een gevaar is voor de openbare orde, de binnenlandse veiligheid, de volksgezondheid of de internationale betrekkingen van een van de lidstaten.

([1])

Biometrie	gezicht	vinger	iris
Niet-invoerbaar (percentage fouten)	n.v.t.	4	7
Foutieve afwijzing	4	2,5	6
Foutieve acceptatie 1 (verificatiefouten)	10	<0,01	<0,001
Foutieve acceptatie 2 (identificatiefouten in bestand groter dan 1 m)	40	0,1	n.v.t.
Foutieve acceptatie 3 (verificatiefouten in bestand van 500)	12	<1	n.v.t.

A.K. Jain et al., *Biometrics: A grand Challenge,* Proceedings of International Conference on Pattern Recognition, Cambridge, UK, August 2004.

([2]) *Biometrics at the frontiers: assessing the impact on Society,* February 2005, Institute for Prospective Technological Studies, DG Joint Research Centre, EC.

([3]) *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data,* Raad van Europa, 2005., blz. 11.

Alle redenen voor weigering moeten, vanwege de gevolgen voor de betrokkene, met grote voorzichtigheid worden gehanteerd. Bovendien zal de in de punten c) en d) bedoelde informatie leiden tot de verwerking van de in artikel 8 van Richtlijn 95/46/EG bedoelde „gevoelige gegevens".

De EDPS vraagt speciale aandacht voor de voorwaarde betreffende de volksgezondheid, die erg vaag is en verwerking van zeer gevoelige gegevens met zich meebrengt. Volgens de toelichting op de artikelen is de verwijzing naar het gevaar voor de volksgezondheid gebaseerd op het „voorstel voor een verordening van de Raad tot vaststelling van een communautaire code betreffende de overschrijding van de grenzen door personen" (COM (2004) 391 def.).

De EDPS weet dat het criterium van de „volksgezondheid" veel gebruikt wordt in de communautaire wetgeving inzake het vrije verkeer van personen en strikt wordt toegepast, zoals blijkt uit Richtlijn 2004/38/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende het recht van vrij verkeer en verblijf op het grondgebied van de lidstaten voor de burgers van de Unie en hun familieleden. Artikel 29 bevat de voorwaarden waaronder er sprake is van een gevaar voor de volksgezondheid: „Enkel potentieel epidemische ziekten zoals gedefinieerd in de relevante instrumenten van de Wereldgezondheidsorganisatie, en andere infectieziekten of besmettelijke parasitaire ziekten kunnen een beperking van vrijheid van verkeer rechtvaardigen, voorzover het gastland beschermende regelingen treft ten aanzien van de eigen onderdanen."

— Er zij echter op gewezen dat het hierboven genoemde voorstel tot nu toe slechts een voorstel is, en dat de voorwaarde inzake het gevaar voor de volksgezondheid kan pas in de VIS-verordening kan worden opgenomen als de communautaire code is aangenomen.

— Voorts moet, als de code is aangenomen, deze reden voor het weigeren van toelating in restrictieve zin worden gelezen. Het voorstel voor de communautaire code is immers op zijn beurt gebaseerd op voornoemde Richtlijn 2004/38/EG.

De EDPS beveelt derhalve aan een verwijzing naar artikel 29 van Richtlijn 2004/38/EG in het voorstel op te nemen om duidelijk te maken dat „gevaar voor de volksgezondheid" in het licht van die bepaling begrepen moet worden. In elk geval mogen de gegevens, gelet op de gevoeligheid ervan, alleen verwerkt worden als er sprake is van een werkelijk bestaand en voldoende ernstig gevaar voor de volksgezondheid.

3.5.2. *Gegevens over andere leden van een groep*

Artikel 2, punt 7, definieert „leden van de groep" als „andere aanvragers met wie de aanvrager samen reist, daaronder begrepen de echtgenoot/echtgenote en de kinderen die de aanvrager vergezellen.". In de toelichting op de artikelen wordt erop gewezen dat de definities in artikel 2 van het voorstel verwijzen naar het Verdrag of naar het Schengenacquis inzake visumbeleid, behalve wat bepaalde termen betreft, zoals „leden van de groep", die specifiek gedefinieerd zijn in de context van deze verordening. Derhalve mag ervan worden uitgegaan dat deze definitie niet overeenkomt met die van collectief visum in artikel 2.1.4 van de Gemeenschappelijke Visuminstructies. In de toelichting op de artikelen is sprake van „aanvragers die in een groep reizen met andere aanvragers, bijv. in het kader van een ADS-overeenkomst, of met familieleden."

De EDPS benadrukt dat er in de verordening een exacte, sluitende definitie van „leden van de groep" gegeven moet worden. Wat het onderhavige voorstel betreft, moet de EDPS opmerken dat de definitie te vaag is, omdat een duidelijke verwijzing naar het Verdrag of het Schengenacquis ontbreekt. Volgens deze formulering kunnen onder „leden van de groep" ook collega's verstaan worden, andere klanten die deelnemen aan een georganiseerde reis van hetzelfde reisbureau, enz. De consequenties zijn ingrijpend:

volgens artikel 5 van de ontwerp-verordening worden de aanvraagdossiers van de leden van de groep aan elkaar gekoppeld.

3.6 **Bewaring van de gegevens**

Artikel 20 van de ontwerp-verordening voorziet in een bewaringstermijn van vijf jaar voor elk aanvraagdossier. Het is een beleidskeuze om in het kader van de communautaire wetgeving een redelijke termijn in acht te nemen.

Er is geen aanwijzing — vooral niet in het licht van de redenen die in de toelichting op de artikelen genoemd worden- om te beweren dat de beleidskeuze die in dit voorstel wordt gemaakt, onredelijk is of onaanvaardbare gevolgen zou hebben, vooropgesteld dat alle passende correctiemechanismen toegepast worden. Dit betekent dat gegevens rechtgezet of verwijderd moeten worden wanneer deze niet langer juist zijn, met name wanneer de betrokkene de nationaliteit van een lidstaat heeft gekregen, of een status heeft verworven die niet vereist dat zijn gegevens nog in het bestand worden bewaard.

Bovendien kunnen gegevens die nog in het bestand zitten, in geen geval gebruikt worden voor een nieuwe beslissing. Sommige redenen voor weigering (met name dat de aanvrager gesignaleerd staat ter fine van weigering van toegang, of een gevaar voor de volksgezondheid is) hebben een beperkte geldigheidsduur. Het feit dat dit op een gegeven moment geldige redenen waren om de toegang te weigeren, mag een nieuwe beslissing niet beïnvloeden. Voor elke nieuwe visumaanvraag moet de gehele situatie opnieuw beoordeeld worden, en dat moet, waar nodig, expliciet in de verordening worden aangegeven.

3.7 **Toegang tot en gebruik van gegevens**

3.7.1. *Opmerkingen vooraf*

De EDPS erkent dat er duidelijk veel zorg besteed is aan de regelgeving voor de toegang tot en het gebruik van de VIS-gegevens. Elke autoriteit heeft toegang tot verschillende soorten gegevens voor verschillende doeleinden. Dat is een goede aanpak, die de EDPS alleen maar kan aanmoedigen. De volgende opmerkingen zijn bedoeld om die aanpak zo breed mogelijk uit te voeren.

3.7.2. *Visumcontrole aan buitengrensposten en op het grondgebied*

Voor de visumcontroles aan de buitengrens vermeldt artikel 16 van de voorgestelde verordening duidelijk de twee precieze doelen:

— „verificatie van de identiteit van de persoon", wat volgens de gegeven definitie een „één op één-vergelijking" inhoudt;

— „verificatie van de echtheid van het visum". Volgens de ICAO-normen kan voor de microchip in het visum een publiek/privaat sleutelsysteem (PKI) gebruikt worden voor de authentificatie.

Beide doelen kunnen verwezenlijkt worden door de bevoegde autoriteiten bij de visumcontroles alleen toegang te verlenen tot de beveiligde microchip. Toegang verschaffen tot het centrale gegevensbestand van het VIS zou in dit specifieke geval buiten proportie zijn. Bij laatstgenoemde optie zouden er meer bij het VIS betrokken autoriteiten ingeschakeld moeten worden, waardoor het risico van misbruik zou kunnen toenemen. Het is waarschijnlijk ook een duurdere optie, omdat het aantal gevallen van beveiligde en gecontroleerde toegang tot het VIS en de behoefte aan speciale opleidingen in verband met deze toegang, ook aanzienlijk zal stijgen.

Voorts zijn er twijfels of de toegang tot de in lid 2 van artikel 16 bedoelde gegevens wel adequaat is. Lid 2, punt a) bepaalt immers dat, als na een eerste controle blijkt dat in het VIS gegevens over de aanvrager zijn opgeslagen (wat in principe het geval moet zijn), de bevoegde autoriteit, uitsluitend met het oog op de verificatie van de identiteit, andere gegevens kan controleren. Deze gegevens hebben betrekking op alle informatie die verband houdt met de aanvraag, namelijk foto's, vingerafdrukken en eerder afgegeven, nietig verklaarde, ingetrokken of verlengde visa.

Indien de verificatie van de identiteit succesvol was, is in het geheel niet duidelijk waarom al die andere gegevens nodig zijn. Die moeten eigenlijk alleen onder bijzondere voorwaarden toegankelijk zijn, als de verificatie mislukt is. In dat geval kunnen de in artikel 16, lid 2, bedoelde gegevens goed gebruikt worden voor een vangnetprocedure waarmee de identiteit van de betrokkene alsnog kan worden vastgesteld. Die gegevens moeten dan niet toegankelijk zijn voor het personeel van elke grenspost, maar alleen, in beperkte mate, voor met moeilijke gevallen belaste ambtenaren.

Tenslotte moet beter omschreven worden welke autoriteiten toegang hebben. Het is met name niet duidelijk wie bedoeld worden met „de autoriteiten die bevoegd zijn controles op het grondgebied van de lidstaat te verrichten". De EDPS neemt aan dat het de autoriteiten betreft die bevoegd zijn controles *op visa* te verrichten: artikel 16 moet in die zin worden gewijzigd.

3.7.3. *Gebruik van gegevens voor de identificatie en terugkeer van illegale immigranten en voor asielaanvragen*

In de in de artikelen 17, 18 en 19 bedoelde gevallen (terugkeer van illegale immigranten en asielaanvragen) wordt het VIS gebruikt voor identificatie. Daarvoor kunnen ook foto's gebruikt worden. Bij de huidige stand van de techniek voor automatische gezichtsherkenning voor zulke uitgebreide IT-systemen zijn foto's echter niet bruikbaar voor identificatie (een-op-veel-vergelijking); ze geven geen betrouwbaar resultaat en kunnen derhalve niet beschouwd worden als voor identificatie bruikbare gegevens.

Derhalve stelt de EDPS met klem voor „foto's" in het eerste deel van deze artikelen te schrappen en in het tweede deel te handhaven (foto's kunnen gebruikt worden om iemands identiteit te verifiëren, maar niet voor identificatie via een uitgebreide gegevensbank).

Een andere optie is artikel 36 zo aan te passen dat de functies voor de verwerking van foto's voor identificatiedoeleinden alleen worden uitgevoerd als de technologie daarvoor betrouwbaar is (mogelijk na raadpleging van het technisch comité).

3.7.4. *Bekendmaking van de autoriteiten die toegang hebben*

Artikel 4 van de ontwerp-verordening bepaalt dat de door de lidstaten aangewezen autoriteiten die toegang hebben tot het VIS in het *Publicatieblad van de Europese Unie* bekendgemaakt worden. Die bekendmaking moet regelmatig (jaarlijks) geschieden, om de wijzigingen in de nationale situatie bij te houden. De EDPS benadrukt dat deze bekendmaking een onontbeerlijk controle-instrument is, zowel op Europees als op nationaal en lokaal niveau.

3.8. **Verantwoordelijkheden**

Het VIS wordt gebaseerd op een gecentraliseerde architectuur met een centraal gegevensbestand waarin alle informatie over visa wordt opgeslagen, terwijl de bevoegde autoriteiten van de lidstaten via de nationale interfaces toegang hebben tot het centrale systeem. Volgens de veertiende en de vijftiende overweging van de ontwerp-verordening is Richtlijn 95/46/EG van toepassing op de verwerking van persoonsgegevens door de lidstaten krachtens deze verordening, en is Verordening (EG) nr. 45/2001 van toepassing op de activiteiten van de Commissie in verband met de bescherming van persoonsgegevens. Zoals in die overwegingen is vermeld, wil het voorstel enkele zaken verduidelijken, onder andere met betrekking tot de verantwoordelijkheid voor het gebruik van gegevens en het toezicht op de gegevensbescherming.

Die punten lijken in feite betrekking te hebben op enkele onderdelen die cruciaal zijn voor het functioneren van de beveiligingsmaatregelen van Richtlijn 95/46/EG en Verordening (EG) nr. 45/2001, die zonder die punten niet uitgevoerd kunnen worden en ook niet volledig met het voorstel overeenkomen. De toepasbaarheid van de nationale wetgeving in het kader van de richtlijn veronderstelt normaal gesproken een verantwoordelijke die in de betrokken lidstaat gevestigd is (artikel 4), terwijl de toepasbaarheid van de verordening afhangt van de verwerking van persoonsgegevens door een communautaire instelling of instantie in het kader van de uitoefening van activiteiten die geheel of gedeeltelijk onder de communautaire wetgeving vallen (artikel 3).

Volgens artikel 23, lid 2, van de ontwerp-verordening worden de gegevens „namens de lidstaten in het VIS verwerkt". Krachtens lid 3 wijst de lidstaat de autoriteit aan die moet worden beschouwd als de voor de verwerking verantwoordelijke in de zin van artikel 2, punt d) van Richtlijn 95/46/EG. Dat lijkt te betekenen dat, volgens de regels van de richtlijn, de Commissie beschouwd moet worden als een verwerker, hetgeen bevestigd wordt in de toelichting op de artikelen. ([1])

Deze formulering neigt ertoe de zeer belangrijke en in feite cruciale rol van de Commissie bij de ontwikkeling en tijdens het normaal functioneren van het systeem te onderstrepen. Het is moeilijk om de rol van de Commissie exact te verbinden met het concept van verantwoordelijke of verwerker; zij is hetzij een verwerker met ongewone bevoegdheden (zoals het ontwerpen van het systeem), hetzij een verantwoordelijke met beperkingen (aangezien de gegevens door de lidstaten ingevoerd en gebruikt worden). De Commissie heeft in het VIS werkelijk -zo moet worden erkend- een rol *sui generis*. ([2])

Het grote belang van die rol moet blijken uit een volledige omschrijving van de taken van de Commissie, en niet gegoten worden in een formulering die niet aan de werkelijkheid beantwoordt, omdat zij te restrictief is, niets aan de werking van het VIS verandert en alleen maar verwarring zaait. Dit is tevens belangrijk met het oog op een samenhangend, efficiënt toezicht op het VIS (zie ook punt 3.11). Derhalve beveelt de EDPS aan lid 2 van artikel 23 te schrappen.

De EDPS benadrukt dat een volledige omschrijving van de taken van de Commissie inzake het VIS nog belangrijker is als de Commissie besluit het beheer aan een ander orgaan toe te vertrouwen. In het 'Financieel Memorandum' bij het voorstel is sprake van de mogelijkheid deze taken over te dragen aan het agentschap voor het beheer van de buitengrenzen. Het is in deze context cruciaal dat de Commissie geen onzekerheid laat bestaan omtrent de grenzen van haar bevoegdheden, zodat haar opvolger weet tot waar hij kan gaan.

3.9. **Beveiliging**

Het beheren en in acht nemen van een optimaal beveiligingsniveau voor het VIS is een absolute voorwaarde voor de vereiste bescherming van de in het bestand opgeslagen persoonsgegevens. Daartoe moeten passende beveiligingsmaatregelen worden getroffen tegen de mogelijke risico's in verband met de infrastructuur van het systeem en de betrokkenen. Deze kwestie komt in verschillende gedeelten van het voorstel aan de orde en vereist enige verbetering.

De artikelen 25 en 26 van het voorstel bevatten maatregelen voor gegevensbeveiliging en geven aan welke soorten misbruik voorkomen moeten worden. Deze bepalingen kunnen echter goed aangevuld worden met maatregelen voor een systematisch toezicht op en verslaggeving over de efficiëntie van de reeds genoemde beveiligingsmaatregelen. De EDPS doet meer specifiek de aanbeveling om bepalingen inzake systematische (zelf)controle van de beveiligingsmaatregelen aan deze artikelen toe te voegen.

Dit houdt verband met artikel 40 van het voorstel dat voorziet in toezicht en evaluatie. Deze moeten niet alleen betrekking hebben op de resultaten, de kosteneffectiviteit en de kwaliteit van de dienstverlening, maar ook op de naleving van de wettelijke eisen, vooral op het gebied van gegevensbescherming. De EDPS beveelt aan het toepassingsgebied van artikel 40 uit te breiden tot het toezicht op en de verslaggeving over de rechtmatigheid van de gegevensverwerking.

In aanvulling op artikel 24, lid 4, punt c) en artikel 26, lid 2, punt e) over het naar behoren aangewezen personeel dat toegang heeft tot de gegevens, moet worden bepaald dat de lidstaten ervoor moeten zorgen dat er exacte gebruikersprofielen beschikbaar zijn (die voor de controles ter beschikking moeten worden gehouden van de nationale toezichtautoriteiten. Naast die gebruikersprofielen moet er een volledige lijst met gebruikersidentiteiten door de lidstaten worden opgesteld en permanent worden bijgehouden. Hetzelfde geldt voor de Commissie: artikel 25, lid 2, punt b) moet derhalve in dezelfde zin worden gewijzigd.

([1]) Zie blz. 37 van het voorstel.

([2]) Hoewel de definitie van „voor de verwerking verantwoordelijke" in Richtlijn 95/46/EG en Verordening (EG) nr. 45/2001 ook de mogelijkheid biedt van meer voor de verwerking verantwoordelijken met verschillende verantwoordelijkheden.

Deze beveiligingsmaatregelen worden aangevuld met waarborgen inzake toezicht en organisatie. Artikel 28 van het voorstel omschrijft onder welke voorwaarden en met welke doelen gegevensverwerkende handelingen geregistreerd moeten worden. Die gegevens worden niet alleen geregistreerd met het oog op het toezicht op de gegevensbescherming en het waarborgen van gegevensbeveiliging, maar ook met het oog op de regelmatige zelfcontrole van het VIS. De verslagen daarover dragen bij aan een efficiënte uitvoering van de taken van de toezichthoudende autoriteiten, zodat de zwakke punten opgespoord kunnen worden en tijdens de eigen controleprocedure onder de loep genomen kunnen worden.

3.10. **Rechten van de betrokkene (de persoon op wie de gegevens betrekking hebben)**

3.10.1 *Informatie aan de betrokkene*

Het is van het grootste belang dat de betrokkene van informatie voorzien wordt. Het is een onontbeerlijke waarborg voor de rechten van het individu. Artikel 30 volgt -wat dat betreft- voornamelijk artikel 10 van Richtlijn 95/46/EG.

Deze bepaling behoeft echter enige wijziging opdat zij beter in het VIS-systeem past. De richtlijn schrijft voor dat bepaalde informatie verstrekt moet worden, maar biedt de mogelijkheid om, indien nodig, meer informatie te geven ([1]). In artikel 30 moeten derhalve de volgende punten worden ingevoegd:

— De betrokkene moet worden geïnformeerd over de voor die gegevens geldende bewaringstermijn.

— Artikel 30, lid 1, punt e) betreft „het recht van toegang tot de hem of haar betreffende gegevens en het recht om deze te corrigeren". Beter ware de vermelding van „het recht van toegang, en het recht om te verzoeken om rectificatie of verwijdering van de gegevens". In dat opzicht moet de betrokkene gewezen worden op de mogelijkheid om de desbetreffende toezichthoudende autoriteit om advies of bijstand te vragen.

— Tenslotte is in artikel 30, lid 1, punt a) sprake van informatie over de identiteit van de voor de verwerking verantwoordelijke en, in voorkomend geval, van degene die hem of haar vertegenwoordigt. Aangezien deze verantwoordelijke altijd gevestigd is op het grondgebied van de Europese Unie, is deze regel overbodig.

3.10.2. *Recht van toegang, recht op rechtzetting en verwijdering van gegevens*

De laatste zin van artikel 31, lid 1, luidt als volgt: „Deze toegang tot gegevens kan enkel door een lidstaat worden verleend.". Aangenomen mag worden dat dit betekent dat toegang tot (of mededeling van) de gegevens niet door de centrale eenheid kan worden gegeven, maar wel door een lidstaat. De EDPS beveelt aan uitdrukkelijk te vermelden dat deze gegevens in iedere lidstaat kunnen worden opgevraagd.

Voorts lijkt de bewoording van deze bepaling tevens in te houden dat toegang niet kan worden geweigerd en zal worden verleend zonder toestemming van de verantwoordelijke lidstaat. Dat zou verklaren waarom de nationale autoriteiten moeten samenwerken om de rechten in de artikelen 31, leden 2, 3 en 4, af te dwingen en niet voor het afdwingen van de rechten in artikel 31, lid 1 ([2]).

3.10.3. *Bijstand van toezichthoudende autoriteiten*

In artikel 33, lid 2, staat dat de nationale toezichthoudende autoriteiten gedurende deze procedure (voor een rechter) verplicht blijven om bijstand en advies te verlenen. De betekenis van dit lid is onduidelijk. De nationale toezichthoudende autoriteiten vatten hun rol tijdens een rechtszaak verschillend op. Dit klinkt alsof zij in de rechtszaal de rol moeten vervullen van raadsman van de eiser, wat in veel landen niet mogelijk is.

([1]) Daarin is sprake van „verdere informatie (…) voorzover die, met inachtneming van de specifieke omstandigheden waaronder de verdere informatie verkregen wordt, nodig is om tegenover de betrokkene een eerlijke verwerking te waarborgen."

([2]) Derhalve zou artikel 31, lid 3, over de samenwerking tussen de nationale autoriteiten bij de uitoefening van de rechten op rechtzetting of verwijdering om wille van de duidelijkheid als volgt kunnen worden gewijzigd: „Indien het *in lid 2 genoemde* verzoek". Voor de in lid 1 genoemde verzoeken (toegang) is geen samenwerking tussen de autoriteiten nodig.

3.11. **Toezicht**

Het voorstel verdeelt de toezichthoudende taak over de nationale toezichthoudende autoriteiten en de EDPS. Dit strookt met de wijze waarop in het voorstel het toepasselijk recht en de verantwoordelijkheden voor de exploitatie en het gebruik van het VIS worden benaderd, en met de noodzaak van een doeltreffend toezicht. Daarom juicht de EDPS deze benadering in de artikelen 34 en 35 toe.

De nationale toezichthoudende autoriteiten zien toe op de rechtmatigheid van de verwerking van persoonsgegevens door de lidstaten, *met inbegrip van de verzending van deze gegevens naar en van het VIS*. De EDPS ziet toe op de activiteiten van de Commissie en ziet er *tevens op toe dat persoonsgegevens rechtmatig tussen de nationale interfaces en het centrale visuminformatiesysteem worden verzonden*. Dit kan leiden tot overlappingen, aangezien zowel de nationale autoriteit als de EDPS verantwoordelijk zijn voor het toezicht op de rechtmatigheid van de verzending van gegevens tussen de nationale interfaces en het centrale visuminformatiesysteem.

Daarom stelt de EDPS voor om artikel 34 zodanig te wijzigen dat duidelijk wordt gesteld dat de nationale toezichthoudende autoriteiten toezien op de rechtmatigheid van de verwerking van persoonsgegevens door de lidstaat, met inbegrip van de verzending van deze gegevens naar en van de nationale interface van het VIS.

Wat betreft het toezicht op het VIS dient ook te worden benadrukt dat de toezichthoudende activiteiten van de nationale toezichthoudende autoriteiten en die van de EDPS tot op zekere hoogte moeten worden gecoördineerd, zodat een toereikend niveau van samenhang en algemene doeltreffendheid wordt bereikt. De verordening moet namelijk op geharmoniseerde wijze worden toegepast en er moet worden toegewerkt naar een gemeenschappelijke aanpak van gemeenschappelijke problemen. Daar kan nog aan worden toegevoegd dat, wat de veiligheid betreft, het niveau van de veiligheid van het VIS (uiteindelijk) wordt bepaald door het veiligheidsniveau van de zwakste schakel van het systeem. Ook in dit verband moet de samenwerking tussen de EDPS en de nationale autoriteiten gestructureerd en versterkt worden. Artikel 35 zou hierover dus een bepaling moeten bevatten waarin staat dat de EDPS op zijn minst eens per jaar een vergadering belegt met alle nationale toezichthoudende autoriteiten.

3.12. **Invoering**

In artikel 36, lid 2, van het voorstel staat: *„De technische maatregelen die nodig zijn voor de invoering van de in lid 1 bedoelde functies worden overeenkomstig de in artikel 39, lid 2, bedoelde procedure goedgekeurd."*. Artikel 39 gaat over een in december 2001 opgericht comité ([1]) dat de Commissie bijstaat en in verscheidene instrumenten is gebruikt.

De technische invoering van de VIS-functies (interacties met de bevoegde autoriteiten en het uniform visummodel) kan een aantal kritieke gevolgen hebben voor de gegevensbescherming. Zo zullen de keuze om al dan niet een microchip in het visum aan te brengen (wat gevolgen zal hebben voor de manier waarop de centrale gegevensbank wordt gebruikt) en de standaard van het formaat dat voor de uitwisseling van biometrische gegevens wordt gebruikt, het daarmee samenhangende gegevensbeschermingsbeleid sturen of bepalen ([2]).

De selectie van de technologieën zal van doorslaggevend belang zijn voor een correcte toepassing van de beginselen van finaliteit en evenredigheid en dus moet hierop worden toegezien. Daarom moeten technologische keuzes met grote gevolgen voor de gegevensbescherming bij voorkeur worden gemaakt middels een verordening, volgens de medebeslissingsprocedure. Alleen dan kan de noodzakelijke politieke controle worden uitgeoefend. In alle andere gevallen met gevolgen voor de gegevensbescherming moet de EDPS de gelegenheid krijgen advies te geven over de keuzes van dit comité.

3.13. **Interoperabiliteit**

Interoperabiliteit is een kritieke en essentiële voorwaarde voor de doeltreffendheid van grootschalige IT-systemen zoals het VIS. De algemene kosten kunnen er consequent door worden teruggedrongen en de voorspelbare overbodigheid van heterogene elementen kan erdoor worden vermeden. Interoperabiliteit kan ook bijdragen aan de doelstelling van een gemeenschappelijk visumbeleid doordat dezelfde procedurele standaard wordt toegepast op alle onderdelen van dit beleid. Het is echter van groot belang onderscheid te maken tussen twee niveaus van interoperabiliteit.

— Interoperabiliteit tussen de lidstaten van de EU is zeer wenselijk. De visumaanvragen die door de autoriteiten van de ene lidstaat worden toegestuurd moeten interoperabel zijn met de aanvragen die de autoriteiten van een andere lidstaat toesturen.

([1]) Verordening (EG) nr. 2424/2001 van de Raad van 6 december 2001 betreffende de ontwikkeling van een Schengeninformatiesysteem van de tweede generatie (SIS II).

([2]) Het voorstel voor een verordening van de Raad tot wijziging van Verordening (EG) nr. 1683/95 (uniform visummodel) van september 2003 bevatte een soortgelijk artikel.

— Interoperabiliteit tussen systemen die voor uiteenlopende doelen zijn ingesteld of met systemen van derde landen is veel minder vanzelfsprekend.

Eén van de beschikbare beschermingen die worden gebruikt om het doel van het systeem af te bakenen en „functieverschuiving" te voorkomen, kan het gebruik van verschillende technologische normen zijn. Voorts moet iedere vorm van interactie tussen twee verschillende systemen terdege worden gedocumenteerd. Interoperabiliteit mag nooit leiden tot een situatie waarin een autoriteit die geen toegang heeft tot bepaalde gegevens en deze niet mag gebruiken, deze toegang kan verkrijgen via een ander informatiesysteem.

In dit verband wil de EDPS verwijzen naar de verklaring van de Raad van 25 maart 2004 over de bestrijding van terrorisme, waarin de Commissie wordt verzocht voorstellen in te dienen voor het versterken van de interoperabiliteit en de synergieën tussen informatiesystemen (SIS, VIS en Eurodac).

Ook wil hij verwijzen naar het debat dat momenteel wordt gevoerd over de vraag welk orgaan in de toekomst kan worden belast met het beheer van de verschillende grootschalige systemen (zie ook punt 3.8 van dit advies).

De EDPS wenst nogmaals te benadrukken dat de invoering van interoperabiliteit niet mag inhouden dat het beginsel van de afbakening van het doel wordt geschonden, en dat ieder voorstel op dit gebied aan hem moet worden voorgelegd.

4. **CONCLUSIES**

4.1. **Algemene punten**

1. De EDPS erkent dat voor de verdere ontwikkeling van een gemeenschappelijk visumbeleid een doeltreffende uitwisseling van relevante gegevens noodzakelijk is. Een van de mechanismen die kunnen zorgen voor een vlotte informatiestroom is het VIS. De EDPS heeft alle aanwijzingen in het EIB zorgvuldig bestudeerd. Hoewel deze aanwijzingen niet geheel doorslaggevend zijn, lijken er genoeg redenen te zijn voor het opzetten van het VIS met als doel het verbeteren van het gemeenschappelijke visumbeleid.

   Dit nieuwe instrument moet echter wel beperkt worden tot het verzamelen en uitwisselen van gegevens, voorzover dit verzamelen en uitwisselen noodzakelijk is voor de ontwikkeling van een gemeenschappelijk visumbeleid en evenredig is met deze doelstelling.

2. De instelling van het VIS kan positieve gevolgen hebben voor andere rechtmatige openbare belangen, maar dit verandert niets aan het doel van het VIS. Daarom moeten alle elementen van het VIS noodzakelijke en evenredige instrumenten zijn om bovenstaand beleidsdoel te bereiken. Bovendien

   — zou routinematige toegang van rechtshandhavingsautoriteiten niet stroken met dit doel.

   — beveelt de EDPS aan in de tekst van artikel 1, lid 2, een duidelijker onderscheid te maken tussen „doel" en „positieve consequenties".

   — mag de invoering van interoperabiliteit met andere systemen niet inhouden dat het beginsel van de afbakening van het doel wordt geschonden.

3. De EDPS erkent de voordelen van het gebruik van biometrische gegevens, maar benadrukt dat dit gebruik grote gevolgen kan hebben en stelt voor het gebruik aan strenge beveiligingsmaatregelen te onderwerpen. Bovendien maken de technische tekortkomingen van vingerafdrukken het nodig dat er vangnetprocedures worden ontwikkeld en in het voorstel worden opgenomen.

4. Dit advies moet vóór de overwegingen in de preambule van de verordening worden genoemd (Gezien het advies ....).

4.2. **Overige punten**

5. Wat betreft de gronden voor weigering van een visum: in het voorstel moet worden verwezen naar artikel 29 van Richtlijn 2004/38/EG om ervoor te zorgen dat „gevaar voor de volksgezondheid" wordt uitgelegd in het licht van dat artikel.

6. Gegevens over leden van een groep hebben een speciale betekenis in het voorstel, daarom moet er een nauwkeurige en sluitende definitie worden gegeven van „leden van de groep".

7. Niets wijst erop dat de beleidskeuze die in dit voorstel wordt gemaakt inzake de termijn voor het bewaren van gegevens onredelijk is of onaanvaardbare gevolgen zou hebben, vooropgesteld dat alle passende correctiemechanismen toegepast worden.

   Verder dient in het voorstel duidelijk te worden gesteld dat persoonsgegevens voor iedere nieuwe visum aanvraag in hun geheel opnieuw moeten worden bekeken.

8. Wat betreft visumcontroles aan de buitengrenzen moet artikel 16 van het voorstel worden gewijzigd, aangezien toegang tot de centrale gegevensbank van het VIS in die gevallen buiten proportie zou zijn. Het volstaat wanneer de bevoegde autoriteiten uitsluitend toegang hebben tot de beschermde microchip om een visum te controleren.

   Bovendien is het, indien de verificatie van de identiteit succesvol was, in het geheel niet duidelijk waarom al die andere gegevens nodig zijn.

9. Met betrekking tot het gebruik van gegevens voor de identificatie en de terugkeer van illegale immigranten en voor asielprocedures: „foto's" moet worden geschrapt uit het eerste deel van de artikelen 17, 18 en 19 en worden gehandhaafd in het tweede deel.

10. Wat de verantwoordelijkheden van de Commissie en de lidstaten betreft: artikel 23, lid 2, moet worden geschrapt.

11. Aan het voorstel moeten bepalingen worden toegevoegd over de systematische (zelf)controle van de beveiligingsmaatregelen. Het toepassingsgebied van artikel 40 moet worden uitgebreid tot toezicht op en verslaglegging over de rechtmatigheid van de verwerking. Bovendien

   — moeten de lidstaten een volledige lijst van gebruikersidentiteiten opstellen en permanent bijwerken. Dit geldt ook voor de Commissie: daarom moet artikel 25, lid 2, onder b), op dezelfde wijze worden aangevuld.

   — wordt in artikel 28 aangegeven onder welke voorwaarden en met welk oogmerk alle gegevensverwerkende handelingen geregistreerd moeten worden. Deze registratie wordt niet alleen bewaard voor toezicht op de gegevensbescherming en voor het waarborgen van gegevensbeveiliging, maar ook met het oog op regelmatige zelfcontrole van het VIS.

12. Inzake de rechten van de betrokkene

   — moet artikel 30 zodanig worden gewijzigd dat de betrokkenen ook moeten worden ingelicht over de bewaringstermijn die voor hun gegevens geldt.

   — moet in artikel 30, lid 1, onder e), komen te staan: „het recht op toegang en het recht om te verzoeken om rechtzetting of verwijdering van de gegevens".

   — moet in artikel 31, lid 1, duidelijk worden gesteld dat bepaalde gegevens in alle lidstaten kunnen worden opgevraagd.

13. Wat betreft toezicht:

— moet artikel 34 zodanig worden gewijzigd dat duidelijk wordt gesteld dat de nationale toezichthoudende autoriteiten toezien op de rechtmatigheid van de verwerking van persoonsgegevens door de lidstaat, inclusief de verzending van deze gegevens van en naar de nationale interface van het VIS.

— moet in artikel 35 staan dat de EDPS op zijn minst eens per jaar een vergadering belegt met alle nationale toezichthoudende autoriteiten.

14. Wat betreft de invoering

— moeten technologische keuzes met grote gevolgen voor gegevensbescherming bij voorkeur worden gemaakt middels een verordening, volgens de medebeslissingsprocedure.

— moet de EDPS in andere gevallen de gelegenheid krijgen advies uit te brengen over de keuzes van het in dit voorstel ingestelde comité.

Brussel, 23 maart 2005.

Peter HUSTINX

De Europese Toezichthouder voor Gegevensbescherming