DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING

ADVIES VAN DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING

— over het voorstel voor een besluit van de Raad betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) (COM(2005) 230 def.);

— het voorstel voor een verordening van het Europees Parlement en de Raad betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) (COM(2005) 236 def.), en

— het voorstel voor een verordening van het Europees Parlement en de Raad betreffende de toegang tot het Schengeninformatiesysteem van de tweede generatie (SIS II) voor de instanties die in de lidstaten belast zijn met de afgifte van kentekenbewijzen van voertuigen (COM(2005) 237 def.)

(2006/C 91/11)

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 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, en met name op artikel 41,

Gezien het verzoek om advies op grond van artikel 28, lid 2, van Verordening (EG) nr. 45/2001 dat op 17 juni 2005 van de Commissie is ontvangen;

HEEFT HET VOLGENDE ADVIES AANGENOMEN:

1. INLEIDING

1.1. Achtergrond

Het Schengeninformatiesysteem (het SIS) is een IT-systeem dat in de EU is opgezet als compenserende maatregel voor de afschaffing van de controles aan de binnengrenzen van het Schengengebied. Het SIS stelt de bevoegde autoriteiten van de lidstaten in staat om informatie uit te wisselen ten behoeve van de controle van personen en voorwerpen aan de buitengrenzen of op het grondgebied, alsmede ten behoeve van de afgifte van visa en verblijfstitels.

De Schengenuitvoeringsovereenkomst is in 1995 als een intergouvernementele overeenkomst in werking getreden. Het SIS, een onderdeel van de Schengenuitvoeringsovereenkomst, werd naderhand bij het Verdrag van Amsterdam in de EU opgenomen.

Een nieuw Schengeninformatiesysteem van de tweede generatie (SIS II) zal in de plaats komen van het huidige systeem, zodat het Schengengebied tot de nieuwe EU-lidstaten kan worden uitgebreid. Er zullen tevens nieuwe functies in het systeem worden ingevoerd. De in een intergouvernementeel kader opgestelde Schengenbepalingen zullen volledig in klassieke Europese rechtsinstrumenten worden omgezet.

Op 1 juni 2005 heeft de Europese Commissie drie voorstellen voor de instelling van SIS II ingediend. Deze zijn:

— een voorstel voor een verordening op basis van titel IV van het EG-Verdrag (visa, asiel, immigratie en andere beleidsterreinen die verband houden met het vrije verkeer van personen), die betrekking zal hebben op de met de eerste pijler (immigratie) verband houdende aspecten van SIS II, hierna „het verordeningsvoorstel" genoemd;

— een voorstel voor een besluit op basis van Titel VI van het EU-Verdrag (politiële en justitiële samenwerking in strafzaken), dat betrekking zal hebben op het gebruik van het SIS voor doeleinden van de derde pijler, hierna „het voorstel voor een besluit" genoemd;

— een voorstel voor een verordening op basis van Titel V (vervoer), dat specifiek betrekking heeft op de toegang tot het SIS van de autoriteiten die belast zijn met de afgifte van kentekenbewijzen; dit voorstel wordt afzonderlijk behandeld (zie punt 4.6).

In dit verband zij erop gewezen dat de Commissie de komende maanden een mededeling zal uitbrengen over interoperabiliteit en grotere synergieën tussen de EU-informatiesystemen (SIS, VIS, Eurodac).

SIS II bestaat uit een centrale gegevensbank, „het centrale Schengeninformatiesysteem" (CS-SIS), waarbij de Commissie zal zorgen voor het operationele beheer in verband met de door elke lidstaat vastgestelde nationale toegangspunten (N-SIS). De Sirene-autoriteiten zorgen voor de uitwisseling van alle aanvullende informatie (niet in SIS II opgeslagen informatie die echter gerelateerd is aan SIS II-signaleringen).

De lidstaten zullen in SIS II gegevens opnemen in verband met personen die met het oog op aanhouding, overlevering of uitlevering worden gezocht, personen die in het kader van een gerechtelijke procedure worden gezocht, personen die moeten worden onderworpen aan onopvallende of gerichte controle, personen aan wie aan de buitengrenzen de toegang moet worden ontzegd, en vermiste of gestolen voorwerpen. Aan de hand van een aantal in het SIS opgenomen gegevens, een zogenaamde „signalering", kan de bevoegde autoriteit een persoon of voorwerp identificeren.

Het SIS II zal nieuwe kenmerken hebben: ruimere toegang tot het SIS (Europol, Eurojust, nationale officieren van justitie, instanties die belast zijn met de afgifte van voertuigkentekenbewijzen), onderlinge koppeling van signaleringen, invoering van nieuwe gegevenscategorieën, met inbegrip van biometrische gegevens (vingerafdrukken en foto's), en een technisch platform dat met het visuminformatiesysteem zal worden gedeeld. Deze nieuwe elementen waren aanleiding voor jarenlange, verhitte discussies over een verschuiving van het doel van het SIS van een controle-instrument naar een meld- en onderzoeksysteem.

1.2. **Algemene kenmerken van de voorstellen**

1. De EDPS is verheugd dat hij op grond van artikel 28, lid 2, van Verordening (EG) nr. 45/2001 is geraadpleegd. Gezien echter het dwingende karakter van artikel 28, lid 2, dient het onderhavige advies in de preambule van de teksten te worden vermeld.

2. De EDPS is om verschillende redenen ingenomen met de voorstellen. De omzetting van een intergouvernementele structuur in Europese rechtsinstrumenten brengt een aantal positieve gevolgen met zich mee: de rechtskracht van de regels met betrekking tot SIS II zal worden verduidelijkt, het Hof van Justitie zal bevoegd zijn voor de uitlegging van het rechtsinstrument van de eerste pijler, het Europees Parlement zal, in ieder geval ten dele, (zij het in een vrij laat stadium) bij SIS II worden betrokken.

3. Bovendien bevatten de voorstellen, wat de inhoud betreft, een groot aantal gegevensbeschermingsbepalingen, waarvan sommige welkome verbeteringen inhouden ten opzichte van de huidige situatie. Met name valt hierbij te denken aan de maatregelen ten gunste van slachtoffers van identiteitsmisbruik, de uitbreiding van Verordening (EG) nr. 45/2001 tot de werkzaamheden van de Commissie in verband met de verwerking van persoonsgegevens uit hoofde van titel VI, en een betere omschrijving van de gronden voor het signaleren van personen ter fine van weigering van toegang.

4. Voorts is duidelijk dat de voorstellen met de grootste zorgvuldigheid zijn opgesteld; ze zijn complex, maar dat is een afspiegeling van de inherente complexiteit van het systeem waarop zij betrekking hebben. De meeste opmerkingen in dit advies zijn bedoeld om bepalingen te verduidelijken of aan te vullen, maar nopen niet tot volledige herwerking van de teksten.

Niettegenstaande deze in het algemeen positieve beoordeling, kan evenwel een aantal bezwaren worden geformuleerd met name aangaande de volgende punten:

1. In tal van opzichten is het niet duidelijk wat de bedoeling van de tekst is; de afwezigheid van een toelichting is zeer betreurenswaardig. Gezien de uiterst complexe aard van deze documenten had een toelichting echter een basisvoorwaarde moeten zijn. De lezer is in sommige gevallen dan ook aangewezen op puur giswerk.

2. Bovendien valt de afwezigheid van een effectbeoordeling alleen maar te betreuren. Dat er al een eerste versie van het systeem bestaat, is geen gegronde reden, omdat beide systemen op tal van punten van elkaar verschillen. Zo had men meer aandacht moeten schenken aan de gevolgen van de invoering van biometrische gegevens.

3. Het wettelijk kader voor gegevensbescherming is zeer complex; het berust op de gecombineerde toepassing van *lex generalis* en *lex specialis*. Zelfs wanneer er specifieke wetgeving wordt uitgewerkt, moet ervoor worden gezorgd dat het bestaande kader voor gegevensbescherming in Richtlijn 95/46/EG en in Verordening (EG) nr. 45/2001 volledig van toepassing blijft. De gecombineerde toepassing van verschillende rechtsinstrumenten mag niet leiden tot discrepanties tussen nationale systemen op fundamentele punten, noch tot een afzwakking van het huidige gegevensbeschermingsniveau.

4. De toegang van tal van nieuwe instanties, die niet strookt met het oorspronkelijke doel, te weten „controle van personen en voorwerpen", moet vergezeld gaan van strengere waarborgen.

5. De voorstellen zijn voor een groot deel gebaseerd op andere rechtsinstrumenten die nog volop worden uitgewerkt (en soms nog niet eens zijn ingediend). De EDPS heeft begrip voor de moeilijkheden die zich voordoen bij het opstellen van wetgeving in complexe en zich voortdurend ontwikkelende omstandigheden; toch acht hij deze werkwijze niet aanvaardbaar in het licht van de gevolgen voor de betrokkenen en de rechtsonzekerheid die een en ander met zich meebrengt.

6. Er heerst enige verwarring over de verdeling van bevoegdheden tussen de lidstaten en de Commissie. Duidelijkheid is niet alleen van het allergrootste belang voor de goede werking van het systeem, maar ook een basisvoorwaarde voor een alomvattend toezicht op het systeem.

1.3. **Structuur van het advies**

De structuur van het advies is als volgt: eerst wordt het wettelijk kader voor SIS II verduidelijkt. Vervolgens wordt het doel van SIS II omschreven, alsmede de fundamentele verschillen ten opzichte van het huidige systeem. Punt 5 bevat opmerkingen over de rol van respectievelijk de Commissie en de lidstaten in verband met de werking van SIS II. Punt 6 heeft betrekking op de rechten van de betrokkene, terwijl punt 7 nader ingaat op het toezicht op nationaal niveau en dat van de EDPS, alsook op de samenwerking tussen de toezichthouders. Punt 8 bevat een aantal opmerkingen en mogelijke wijzigingen in verband met beveiliging; de punten 9 en 10 betreffen respectievelijk de comitologie en de interoperabiliteit. Tenslotte zijn de belangrijkste conclusies voor elk punt vervat in een samenvatting van conclusies.

2. **WETTELIJK KADER**

2.1. **Kader voor gegevensbescherming voor SIS II**

De voorstellen verwijzen, wat het wettelijk kader voor gegevensbescherming betreft, naar Richtlijn 95/46/EG, Verdrag 108 en Verordening (EG) nr. 45/2001. Ook andere instrumenten zijn relevant.

Ter verduidelijking van deze context en van de belangrijkste referentiepunten voor onze beoordeling is het dienstig om op het volgende te wijzen:

— Het recht op eerbiediging van privéleven is in Europa gewaarborgd sinds de aanneming, in 1950, van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna „EVRM" genoemd) door de Raad van Europa. Artikel 8 EVRM heeft betrekking op „het recht op eerbiediging van privéleven, familie- en gezinsleven".

  Overeenkomstig artikel 8, lid 2, is inmenging van enig openbaar gezag in de uitoefening van dit recht alleen toegestaan, voorzover „bij de wet is voorzien" en „in een democratische samenleving noodzakelijk is" voor de bescherming van wezenlijke 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.

— Het recht op eerbiediging van privéleven en op bescherming van persoonsgegevens is meer recentelijk verankerd in de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie. Overeenkomstig artikel 52 van het Handvest wordt erkend dat deze rechten kunnen worden beperkt, mits soortgelijke voorwaarden zijn vervuld als die welke gelden voor artikel 8 EVRM.

— Artikel 6, lid 2, van het EU-Verdrag bepaalt dat de Unie de grondrechten eerbiedigt, zoals die worden gewaarborgd door het EVRM.

De drie teksten die uitdrukkelijk van toepassing zijn op de voorstellen voor SIS II zijn de volgende:

— Verdrag nr. 108 van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (hierna „*Verdrag 108*" genoemd), bevat fundamentele beginselen voor de bescherming van personen met betrekking tot de verwerking van persoonsgegevens. Alle lidstaten hebben Verdrag 108 bekrachtigd. Het geldt tevens voor op politieel en justitieel gebied verrichte activiteiten. Verdrag 108 is momenteel de gegevensbeschermingsregeling die op het SIS van toepassing is, samen met Aanbeveling R(87) 15 van het Comité van ministers van de Raad van Europa tot regeling van het gebruik van persoonsgegevens op politieel gebied.

— Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB L 281 van 23.11.1995, blz. 31). Deze richtlijn wordt hierna „*Richtlijn 95/46/EG*" genoemd. Opgemerkt zij dat de nationale wetgeving ter uitvoering van de richtlijn in de meeste lidstaten tevens betrekking heeft op gegevensverwerking op politieel en justitieel gebied.

— 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 persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (PB L 8 van 12.1.2001, blz. 1.) Deze verordening wordt hierna „*Verordening 45/2001*" genoemd.

De uitlegging van Richtlijn 95/46/EG en Verordening (EG) nr. 45/2001 moet ten dele berusten op de rechtspraak van het Europees Hof voor de Rechten van de Mens uit hoofde van het EVRM. Met andere woorden, de richtlijn en de verordening moeten in het licht van de grondrechten worden uitgelegd, voorzover zij betrekking hebben op verwerking van persoonsgegevens die afbreuk kan doen aan de fundamentele vrijheden, met name het recht op persoonlijke levenssfeer. Dit vloeit ook voort uit de rechtspraak van het Hof van Justitie van de Europese Gemeenschappen ([1]).

([1]) In dit verband zij verwezen naar het arrest van het Hof van Justitie in de zaken van Österreichischer Rundfunk en anderen (gevoegde zaken C-465/00, C-138/01 en C-139/01, arrest van 20 mei 2003, in voltallige zitting gewezen, 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 Europees Mensenrechtenverdrag leidde het Hof een aantal criteria af die moeten worden gehanteerd bij de toepassing van Richtlijn 95/46/EG, voorzover deze richtlijn beperkingen op het recht op eerbiediging van de privacy mogelijk maakt.

Op 4 oktober 2005 heeft de Commissie een voorstel ingediend 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 (hierna „*ontwerp-kaderbesluit*" genoemd) ([1]). Dit kaderbesluit is bedoeld ter vervanging van Verdrag 108 als referentiewetgeving voor het ontwerp-besluit inzake SIS II, dat in dat verband waarschijnlijk van invloed zal zijn op de gegevensbeschermingsregeling (zie punt 2.2.5).

2.2. **Wettelijke gegevensbeschermingsregeling voor SIS II**

2.2.1. *Algemene opmerking*

De wettelijke basis voor SIS II bestaat uit afzonderlijke instrumenten; dit „doet" evenwel „geen afbreuk aan het beginsel dat SIS II één informatiesysteem vormt, dat als zodanig moet functioneren", zoals in de overwegingen wordt gesteld. „Een aantal bepalingen van deze instrumenten moet bijgevolg identiek zijn".

De structuur van beide documenten is in wezen dezelfde; de hoofdstukken I-III zijn nagenoeg identiek. Dat SIS II moet worden beschouwd als één informatiesysteem met twee verschillende rechtsgrondslagen, komt ook tot uiting in de — veeleer complexe — gegevensbeschermingsregeling.

De gegevensbeschermingsregeling wordt deels bepaald in de voorstellen zelf, als „*lex specialis*", en aangevuld met een referentiewetgeving („*lex generalis*") die per sector verschilt (Commissie, lidstaten in het kader van de eerste pijler, lidstaten in het kader van de derde pijler).

Deze structuur werpt de vraag op hoe moet worden omgesprongen met gespecialiseerde regels in hun relatie tot algemene regels. In dit geval beschouwt de EDPS de specifieke regel als de toepassing van de algemene regel. Bijgevolg moet de *lex specialis* altijd sporen met de *lex generalis*; de *lex specialis* is een nadere uitwerking (of complementering) van de *lex generalis*, maar wordt niet als een uitzondering op die regels beschouwd.

Met betrekking tot de vraag welke regel in specifieke gevallen moet worden toegepast, geldt het beginsel dat de *lex specialis* voorrang heeft. Bij ontstentenis of onduidelijkheid van de *lex specialis* moet naar de *lex generalis* worden verwezen.

Overeenkomstig de hierboven geschetste structuur zijn er drie verschillende combinaties van *lex generalis* en *lex specialis* mogelijk. Een en ander kan als volgt worden samengevat.

2.2.2. *Toepasselijke regeling voor de Commissie*

Op de Commissie is Verordening (EG) nr. 45/2001 van toepassing, ook wat de rol van de EDPS betreft, ongeacht of de werkzaamheden in het kader van de eerste (verordeningsvoorstel), dan wel derde pijler (voorstel voor een besluit) worden verricht. Overweging 21 van het voorgestelde besluit luidt als volgt: „Verordening (EG) nr. 45/2001 (…) is van toepassing op de verwerking van persoonsgegevens door de Commissie, voorzover die verwerking plaatsvindt ten behoeve van de uitvoering van werkzaamheden die geheel of gedeeltelijk onder de werkingssfeer van het Gemeenschapsrecht vallen. De verwerking van persoonsgegevens in het kader SIS II valt gedeeltelijk onder de werkingssfeer van het Gemeenschapsrecht."

Hiervoor zijn praktische redenen: het zou inderdaad uiterst moeilijk zijn om, wat de Commissie betreft, te bepalen of de gegevens worden verwerkt in het kader van werkzaamheden die onder de wetgeving van de eerste dan wel de derde pijler vallen.

Bovendien is de toepassing van één rechtsinstrument op alle werkzaamheden van de Commissie in het kader van SIS II niet alleen logischer uit praktisch oogpunt, maar komt die ook de consistentie ten goede (door te zorgen voor, overeenkomstig overweging 21 van het verordeningsvoorstel, „de coherente en homogene toepassing van de regels inzake de bescherming van de fundamentele rechten en vrijheden van personen in verband met de verwerking van persoonsgegevens"). Het verheugt de EDPS dan ook dat de Commissie erkent dat Verordening (EG) nr. 45/2001 van toepassing is op alle gegevensverwerkingsactiviteiten van de Commissie in het kader van SIS II.

2.2.3. *Toepasselijke regeling voor de lidstaten*

Voor de lidstaten is de situatie complexer. De verwerking van persoonsgegevens binnen de toepassing van het verordeningsvoorstel wordt beheerst door het verordeningsvoorstel zelf, alsmede door Richtlijn 95/46/EG. Uit de redactie van overweging 14 van het verordeningsvoorstel blijkt heel duidelijk dat de richtlijn moet worden beschouwd als *lex generalis*, terwijl de SIS II-verordening als *lex specialis* moet worden aangemerkt. De gevolgen daarvan worden hieronder toegelicht.

Wat het voorstel voor een besluit betreft, is Verdrag 108 het rechtsinstrument inzake gegevensbescherming dat als referentie (*lex generalis*) dient, wat ertoe kan leiden dat de gegevensbeschermingsregelingen voor de eerste en de derde pijler op een aantal punten in aanzienlijke mate van elkaar verschillen.

2.2.4. *Impact op het gegevensbeschermingsniveau*

Bij wijze van algemene kanttekening bij deze gegevensbeschermingsarchitectuur wijst de EDPS op het volgende:

— De toepassing van het verordeningsvoorstel als *lex specialis* van Richtlijn 95/46/EG (en, in dezelfde zin, de toepassing van het voorstel voor een besluit als *lex specialis* van Verdrag 108) mag er geenszins toe leiden dat het gegevensbeschermingsniveau uit hoofde van de richtlijn of het verdrag wordt afgezwakt. De EDPS zal daartoe strekkende aanbevelingen doen (zie bijvoorbeeld het recht op rechtsmiddelen).

([1]) COM(2005) 475 def.

— Evenzo mag de gecombineerde toepassing van rechtsinstrumenten niet tot gevolg hebben dat het in de Schengenuitvoeringsovereenkomst gewaarborgde gegevensbeschermingsniveau wordt verlaagd (zie bijvoorbeeld onderstaande opmerkingen over artikel 13 van Richtlijn 95/46/EG).

— De toepassing van twee verschillende instrumenten, hoe noodzakelijk ook in het licht van het Europese rechtskader, mag niet leiden tot ongerechtvaardigde discrepanties tussen de gegevensbeschermingsregelingen die, afhankelijk van het soort gegevens dat wordt verwerkt, op de betrokkenen van toepassing zijn. Dit moet zoveel mogelijk worden vermeden. Onderstaande aanbevelingen zijn tevens bedoeld om de consistentie zoveel mogelijk te verbeteren (zie bijvoorbeeld de bevoegdheden van de nationale controleautoriteiten).

— Het rechtskader is zo complex dat er wellicht enige verwarring zal ontstaan bij de praktische toepassing ervan. In sommige gevallen is de interactie tussen *lex generalis* en *lex specialis* onduidelijk, en zou het dienstig zijn om een en ander in de voorstellen te verduidelijken. Bovendien is het voorstel van de GCA Schengen vervat in haar „advies over de voorgestelde rechtsgrondslag voor SIS II" (27 september 2005), te weten het opstellen van een vademecum met alle rechten betreffende SIS II en met een duidelijke hiërarchie van de toepasselijke wetgeving, tegen de achtergrond van dit complexe rechtskader zeer dienstig.

Tenslotte wordt met dit advies een hoog niveau van gegevensbescherming, samenhang en duidelijkheid beoogd, zodat de betrokkene voldoende rechtszekerheid kan worden geboden.

2.2.5. *Impact van het ontwerp-kaderbesluit op gegevensbescherming in de derde pijler*

Verdrag 108 zal als referentie-instrument voor het ontwerpbesluit inzake SIS II op het gebied van gegevensbescherming worden vervangen door het kaderbesluit inzake gegevensbescherming in de derde pijler ([1]). Dat wordt in het voorstel niet vermeld, maar vloeit voort uit het voorgestelde kaderbesluit. Artikel 34, lid 2, luidt als volgt: „Iedere verwijzing naar Verdrag 108 van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, moet worden gelezen als een verwijzing naar dit kaderbesluit". De EDPS zal de komende weken advies uitbrengen over het ontwerp-kaderbesluit; in onderhavig advies wordt dan ook niet nader ingaan op de inhoud ervan. Telkens wanneer de toepassing van het kaderbesluit een aanzienlijke invloed kan hebben op de gegevensbeschermingsregeling voor SIS II, zal dat worden vermeld.

([1]) Het kaderbesluit zal ook in de plaats komen van de algemene gegevensbeschermingsregeling van de Schengenuitvoeringsovereenkomst (artikelen 126 tot en met 130). Deze regeling is niet van toepassing op het SIS.

2.2.6. *Toepassing van artikel 13 van Richtlijn 95/46/EG en van artikel 9 van Verdrag 108*

Artikel 13 van Richtlijn 95/46/EG en artikel 9 van Verdrag 108 voorzien in de mogelijkheid voor de lidstaten om wettelijke maatregelen te treffen ter beperking van de reikwijdte van de in de deze artikelen bedoelde rechten en plichten, indien dat noodzakelijk is ter waarborging van andere wezenlijke belangen (bijvoorbeeld de veiligheid van de staat, de landsverdediging, de openbare veiligheid) ([2]).

In de overwegingen van zowel het verordeningsvoorstel als het voorstel voor een besluit wordt gesteld dat deze mogelijkheid door de lidstaten zou kunnen worden gebruikt bij de uitvoering van de voorstellen op nationaal niveau. In dit geval dient een dubbele test te worden gedaan: de toepassing van artikel 13 van Richtlijn 95/46/EG moet in overeenstemming zijn met artikel 8 EVRM en mag niet leiden tot een afzwakking van de huidige gegevensbeschermingsregeling.

Dat is des te belangrijker in het geval van SIS II, omdat het systeem voorspelbaar moet zijn. Aangezien de lidstaten gegevens delen, moet er een mogelijkheid zijn om met redelijke zekerheid te vernemen hoe deze op nationaal niveau zullen worden verwerkt.

In dat verband is er met name één element dat zorgen baart, omdat de voorstellen zouden leiden tot een verlaging van het huidige gegevensbeschermingsniveau. Artikel 102 van de Schengenuitvoeringsovereenkomst voorziet in een systeem waarbij het gebruik van gegevens strikt geregeld en beperkt is, zelfs in de nationale wetgeving („Gebruik dat in strijd is met het bepaalde in de leden 1 tot en met 4 wordt naar nationaal recht aangemerkt als afwijking van doelbinding"). Zowel Richtlijn 95/46/EG als Verdrag 108 bepalen evenwel dat uitzonderingen, onder meer op het beginsel van de beperking van het doel, in het nationaal recht kunnen worden opgenomen. Dat zou echter een discrepantie inhouden ten opzichte van het huidige, in de Schengenuitvoeringsovereenkomst vervatte systeem, waarbij het nationaal recht niet kan afwijken van het kernbeginsel van de beperking van het doel en van het gebruik.

De aanname van het kaderbesluit zou daar niets aan veranderen: het probleem is er veeleer in gelegen het strikte beginsel van de beperking van het doel bij de verwerking van SIS II-gegevens te handhaven, dan ervoor te zorgen dat de gegevens overeenkomstig het kaderbesluit worden verwerkt.

([2]) Een lidstaat die gebruik maakt van deze mogelijkheid om de rechten te beperken, kan dat alleen met inachtneming van artikel 8 EVRM, zoals eerder vermeld.

De EDPS stelt voor om in de SIS II-voorstellen (namelijk in artikel 21 van het verordeningsvoorstel en in artikel 40 van het voorstel voor een besluit) een bepaling op te nemen in de trant van artikel 102, lid 4, van de Schengenuitvoeringsovereenkomst, ter beperking van de mogelijkheid voor de lidstaten om te voorzien in gebruik van gegevens waarin de SIS II-teksten niet voorzien. Een andere mogelijkheid bestaat erin om in het voorstel voor een besluit en in het verordeningsvoorstel de werkingssfeer van de uitzonderingen uit hoofde van artikel 13 van de richtlijn en artikel 9 van het verdrag uitdrukkelijk te beperken, door bijvoorbeeld te bepalen dat de lidstaten alleen het recht van toegang en informatie kunnen beperken, maar niet het beginsel van de kwaliteit van de gegevens.

3. **DOEL**

Luidens artikel 1 van beide documenten („Instelling en algemene doelstelling van SIS II") wordt SIS II ingesteld om „de bevoegde autoriteiten van de lidstaten in staat te stellen samen te werken door informatie uit te wisselen met het oog op controles van personen en voorwerpen", en „bij te dragen aan de handhaving van een hoog niveau van zekerheid in een ruimte zonder controles aan de binnengrenzen tussen de lidstaten".

Het doel van SIS II wordt in eerder algemene bewoordingen aangegeven. Bovengenoemde bepalingen zijn geen precieze indicatie van wat onder deze doelstelling wordt verstaan.

De doelstelling van SIS II lijkt veel ruimer dan de doelstelling van het huidige SIS, zoals vervat in artikel 92 van de Schengenuitvoeringsovereenkomst, dat specifiek verwijst naar „(…) signaleringen van personen en voorwerpen …bij de uitoefening…van grenscontroles … en andere politie- en douanecontroles (…), alsmede (voorzover het de in artikel 96 bedoelde categorie van signaleringen betreft) ten behoeve van de visumverleningsprocedure, de afgifte van verblijfstitels en de toepassing van het vreemdelingenrecht (…)".

De ruimere doelstelling vloeit tevens voort uit de invoering in SIS II van nieuwe functies en toegangsmogelijkheden die niet stroken met het oorspronkelijke doel van controles van personen en voorwerpen, maar veeleer passen bij een onderzoeksinstrument. In het bijzonder wordt voorzien in toegang voor autoriteiten die de SIS II-gegevens zullen gebruiken voor hun eigen doeleinden, dus niet ter verwezenlijking van de SIS II-doeleinden (zie hieronder); koppeling van signaleringen wordt veralgemeend, terwijl dit een typisch kenmerk is van een politieel onderzoeksinstrument.

Er rijzen ook vragen bij de biometrische zoekmachine die de komende jaren zal worden ontwikkeld, en die het mogelijk zal maken in het systeem opzoekingen te doen die de noden van een controlesysteem overstijgen.

Concluderend: de voorstellen hebben een veel ruimer doel dan het bestaande kader. Dit vergt aanvullende waarborgen. In dat verband zal de EDPS zich in zijn analyse niet zozeer richten op de ruime definitie in artikel 1 als dusdanig, maar op de functies en andere elementen van SIS II.

4. **BELANGRIJKE WIJZIGINGEN IN SIS II**

In dit hoofdstuk wordt vooreerst nader ingegaan op de nieuwe elementen van SIS II, namelijk de invoering van biometrische gegevens, het nieuwe concept van toegang, met bijzondere aandacht voor de toegang van Europol en Eurojust, de autoriteiten die belast zijn met de afgifte van kentekenbewijzen, de koppeling van signaleringen en de toegang van verschillende autoriteiten tot immigratiegegevens.

4.1. **Biometrische gegevens**

In de SIS II-voorstellen wordt de mogelijkheid geïntroduceerd om een nieuwe categorie gegevens te verwerken, die specifieke aandacht verdient: biometrische gegevens. Zoals reeds werd benadrukt in het advies van de EDPS over het visuminformatiesysteem, vergt de gevoelige aard van biometrische gegevens specifieke waarborgen, die niet in de SIS II-voorstellen zijn opgenomen ([1]).

In het algemeen zij opgemerkt dat de tendens om biometrische gegevens te gebruiken in EU- informatiesystemen (VIS, EURODAC, Informatiesysteem voor rijbewijzen enz.), steeds sterker wordt, maar niet vergezeld gaat van een zorgvuldige bestudering van de daaraan verbonden risico's en de vereiste waarborgen. Deze noodzaak van nadere bestudering is ook benadrukt in de recente resolutie over biometrische gegevens van de Internationale Conferentie van de functionarissen voor de gegevensbescherming in Montreux ([2]). Tot dusverre was de meerwaarde voor de ontwikkeling van normen uitsluitend gelegen in de grotere interoperabiliteit van systemen, niet in de verbetering van de kwaliteit van biometrische processen.

Het zou dienstig zijn om een aantal gemeenschappelijke verplichtingen of vereisten in verband met de specifieke kenmerken van die gegevens vast te stellen, alsmede een gemeenschappelijke methodologie voor de vervulling ervan.

([1]) Advies van de EDPS van 23 maart 2005 over 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 (punt 3.4.2).

([2]) 27e Internationale Conferentie van de functionarissen voor de gegevensbescherming en de bescherming van de persoonlijke levenssfeer van 16 september 2005 te Montreux; Resolutie over het gebruik van biometrische gegevens in paspoorten, identiteitskaarten en reisdocumenten.

Deze gemeenschappelijke vereisten zouden met name de volgende elementen kunnen bevatten (de noodzaak daarvan wordt geïllustreerd door de SIS II-voorstellen):

— **Gerichte effectbeoordeling:** De voorstellen zijn niet onderworpen aan een effectbeoordeling van het gebruik van biometrische gegevens ([1]).

— **Nadruk op scholing:** Er wordt niet nader ingegaan op de bron van de biometrische gegevens en de wijze waarop deze zullen worden verzameld. Scholing vormt een kritieke stap in het algehele proces van biometrische identificatie, en mag niet uitsluitend worden bepaald in bijlagen of verdere besprekingen in subgroepen, omdat scholing een rechtstreekse invloed zal hebben op het eindresultaat van het proces, dat wil zeggen de hoogte van het foutieve afwijzingspercentage of foutieve aanvaardingspercentage.

— **Nadruk op het niveau van accuraatheid:** Het gebruik van biometrische gegevens voor identificatie (vergelijking één/vele), dat in het voorstel wordt aangemerkt als een toekomstige implementatie van een zoekmachine voor biometrische gegevens, ligt moeilijker, omdat de resultaten van dit proces minder accuraat zijn dan wanneer de biometrische gegevens voor authentificatie of controle (vergelijking één/één) worden gebruikt. Biometrische identificatie mag dan ook niet de enige wijze van identificatie of de enige toegangssleutel tot verdere informatie zijn.

— **Vangnetprocedures:** Er moeten onmiddellijk beschikbare vangnetprocedures komen om de waardigheid te eerbiedigen van personen die verkeerd hadden kunnen worden geïdentificeerd, en om te vermijden dat de last van tekortkomingen van het systeem op hen wordt overgedragen.

Gebruik van biometrische gegevens zonder degelijke, voorafgaande beoordeling komt neer op overwaardering van de betrouwbaarheid van biometrische gegevens. Biometrische gegevens zijn „levende" gegevens die evolueren in de tijd; de in de gegevensbank opgeslagen monsters zijn slechts een momentopname van een dynamisch element. Het permanente karakter ervan is niet absoluut en dient te worden getoetst. Aangezien de accuraatheid van biometrische gegevens nimmer absoluut zal zijn, dient zij altijd in een juiste verhouding te worden geplaatst ten opzichte van andere elementen.

([1]) De beoordeling zou kunnen worden gebaseerd op de zogenaamde zeven pijlers van biometrische wijsheid in „*Biometrics at the frontiers: Assessing the impact on Society*", IPTS, DG GCO, EUR 21585 EN, deel 1.2, blz. 32.

Het mogelijke gebruik van SIS II-gegevens voor onderzoeksdoeleinden brengt voor de betrokkene ernstige risico's met zich mee, wanneer men biometrisch bewijsmateriaal een (al te) belangrijke rol laat spelen, zoals eerder is aangetoond ([2]).

In de voorstellen zou dan ook ruimte moeten zijn voor erkenning van en bewustmaking omtrent de reële mogelijkheden van het gebruik van biometrische gegevens voor identificatiedoeleinden.

4.2. **Toegang tot SIS II-gegevens**

4.2.1 *Een nieuwe visie op toegang*

De autoriteiten die toegang hebben tot de SIS-gegevens, worden voor elke signalering aangegeven. In beginsel wordt een dubbele test verricht, voordat toegang tot de SIS-gegevens wordt verleend: de autoriteiten moet toegang worden verleend in volledige overeenstemming met het algemene doel van het SIS en met het specifieke doel van elke signalering.

Dit vloeit voort uit de definitie van „signalering", zowel in het verordeningsvoorstel als in het voorstel voor een besluit (art. 3, lid 1, punt a), van beide instrumenten: „*signalering": een in SIS II opgenomen reeks gegevens aan de hand waarvan de bevoegde autoriteiten een persoon of een voorwerp kunnen identificeren met het oog op het nemen van een specifieke maatregel)*. In artikel 39, lid 3, van het voorstel voor een besluit wordt dit nog versterkt door de bepaling dat „*de in lid 1 bedoelde gegevens uitsluitend worden gebruikt ter identificatie van een persoon met het oog op de vaststelling van een specifieke maatregel overeenkomstig dit besluit*". In dat verband heeft SIS II nog altijd de kenmerken van een hit/no-hit systeem, waarbij elke signalering wordt opgenomen met een specifiek doel (overlevering, weigering van toegang enz.).

Voor de autoriteiten die toegang hebben tot de SIS-gegevens, is er een feitelijke beperking van het gebruik van deze gegevens, omdat zij in beginsel alleen toegang kunnen krijgen tot de gegevens met het oog op het nemen van een specifieke maatregel.

Enkele van de in de voorstellen genoemde toegangsmogelijkheden druisen evenwel in tegen deze logica: zij hebben immers tot doel om de autoriteiten informatie te verschaffen, niet om deze in staat te stellen een persoon te identificeren en de in de signalering genoemde maatregel te nemen.

([2]) In juni 2004 belandde een advocaat uit Portland (VS) twee weken in de gevangenis omdat de FBI zijn vingerafdruk koppelde aan een vingerafdruk die bij de terroristische bomaanslag in Madrid werd gevonden (op het plastic zakje dat de detonator bevatte). Uiteindelijk werd aangetoond dat de koppeling onjuist was en tot een foutieve interpretatie leidde.

Meer bepaald gaat het om de volgende toegangsmogelijkheden:

— toegang van de voor asiel bevoegde autoriteiten tot immigratiegegevens;

— toegang van de voor toekenning van de vluchtelingenstatus bevoegde autoriteiten tot immigratiegegevens;

— toegang van Europol tot signaleringen ter fine van uitlevering en onopvallende controle en signaleringen inzake gestolen documenten, met het oog op inbeslagneming;

— toegang van Eurojust tot gegevens inzake uitlevering en lokalisatie.

Al deze autoriteiten hebben dezelfde kenmerken met betrekking tot de SIS II-gegevens:

zij zijn niet in staat om de in de signalering genoemde specifieke maatregel te nemen. Er wordt hun toegang verleend als bron van informatie voor hun eigen doeleinden.

Zelfs bij deze autoriteiten dient een onderscheid te worden gemaakt tussen diegenen die toegang hebben voor hun eigen doeleinden, maar met een eerder specifieke doelstelling, en diegenen (namelijk Europol en Eurojust) voor wie het doel van de toegang helemaal niet gespecificeerd is. Zo hebben de voor asiel bevoegde autoriteiten toegang voor een specifiek doel, zelfs wanneer dat niet het in de signalering genoemde doel is. Zij kunnen toegang krijgen tot immigratiegegevens „om vast te stellen of een asielzoeker illegaal in een andere lidstaat heeft verbleven". Europol en Eurojust hebben echter toegang tot de in bepaalde categorieën van signaleringen opgenomen gegevens, „die nodig is om hun taken te vervullen"

Samengevat: er wordt toegang tot SIS II-gegevens verleend in drie gevallen:

— toegang met het oog uitvoering van de signalering;

— in de voorstellen welomschreven toegang voor een ander doel dan SIS II;

— niet duidelijk omschreven toegang voor een ander doel dan SIS II.

De EDPS is van oordeel dat, hoe algemener het doel van de toegang is, des te strikter de te vervullen waarborgen moeten zijn. De algemene waarborgen worden hieronder nader toegelicht; vervolgens wordt nader ingegaan op de specifieke situatie van Europol en Eurojust.

4.2.2 *Voorwaarden voor toegang*

1. Toegang kan in ieder geval alleen worden verleend wanneer deze verenigbaar is met het algemene doel van SIS II, en overeenstemt met de rechtsgrondslag.

Dat betekent in de praktijk dat de toegang tot immigratiegegevens uit hoofde van het verordeningsvoorstel moet strekken tot de uitvoering van het beleid op het gebied van het vrije verkeer van personen dat deel uitmaakt van het Schengenacquis.

Evenzo moet de toegang tot signaleringen uit hoofde van het besluit strekken tot ondersteuning van de operationele samenwerking van justitie en politie in strafzaken.

In dat verband attendeert de EDPS op het hoofdstuk dat betrekking heeft op de toegang tot SIS II van de diensten die belast zijn met de afgifte van kentekenbewijzen (zie punt 4.6).

2. De noodzaak van toegang tot SIS II-gegevens moet worden aangetoond, alsmede de onmogelijkheid dan wel de grote moeilijkheid om de gegevens met andere, minder ingrijpende middelen te verkrijgen. Dat had moeten gebeuren in een toelichting; de afwezigheid daarvan wordt, zoals eerder werd opgemerkt, ten zeerste betreurd.

3. Het beoogde gebruik van de gegevens moet uitdrukkelijk en restrictief worden omschreven.

Zo hebben de voor asiel bevoegde autoriteiten toegang tot immigratiegegevens „om vast te stellen of een asielzoeker illegaal in een andere lidstaat heeft verbleven". Europol en Eurojust hebben echter toegang tot de in bepaalde categorieën van signaleringen opgenomen gegevens, „die nodig is om hun taken te vervullen". Dat is niet voldoende gedetailleerd (zie hieronder).

4. De voorwaarden voor toegang moeten welomschreven en restrictief zijn. Met name mogen alleen de diensten binnen de organisaties die zich bezighouden met SIS II-gegevens, toegang krijgen tot deze gegevens. Deze verplichting, als vervat in artikel 40 van het voorstel voor een besluit en in artikel 21, lid 2, van het verordeningsvoorstel, zou moeten worden aangevuld met een verplichting voor de nationale autoriteiten om een lijst bij te houden van de personen die toegang hebben tot SIS II. Hetzelfde geldt voor Europol en Eurojust.

5. Dat deze autoriteiten toegang tot SIS II-gegevens krijgen, kan nimmer een grond zijn voor opneming of behoud in het systeem van gegevens die niet dienstig zijn voor de specifieke signalering waarop zij betrekking hebben. Nieuwe categorieën van gegevens mogen niet worden toegevoegd omdat zij andere informatiesystemen ten goede zouden komen. Zo voorziet artikel 39 van het voorstel voor een besluit in de opneming van gegevens betreffende de signalerende autoriteit in signaleringen. Deze gegevens zijn niet nodig om een maatregel (aanhouding, onopvallende controle, enz.) uit te voeren; de enige reden waarom zij zouden kunnen worden opgenomen, is om er Europol of Eurojust van te laten profiteren. De beginselen voor de verwerking van deze gegevens moeten duidelijk worden uiteengezet.

6. De bewaartermijn van de gegevens mag niet worden verlengd, wanneer dat niet nodig is voor het doel waarvoor de gegevens zijn opgenomen. Dat betekent dat, zelfs wanneer Europol of Eurojust toegang heeft tot deze gegevens, zulks niet voldoende grond is om deze in het systeem te handhaven (zodra een gezochte persoon bijvoorbeeld is uitgeleverd, moeten de gegevens worden verwijderd, zelfs indien deze nuttig zouden kunnen zijn voor Europol). Ook hier is zorgvuldig toezicht geboden om ervoor te zorgen dat de nationale autoriteiten zich daaraan houden.

4.2.3 *Toegang van Europol en Eurojust*

a. *Gronden voor toegang*

Over de toegang van Europol en Eurojust tot bepaalde SIS-gegevens is reeds gesproken voordat deze werden opgenomen in het besluit van de Raad van 24 februari 2005 [1]. Van alle autoriteiten die voor hun eigen doeleinden toegang hebben, genieten zij de meest ruime toegang. Hoewel het gebruik van deze gegevens wordt omschreven in hoofdstuk XII van het besluit, zijn de gronden voor toegang niet voldoende uitgewerkt. Dat geldt des te meer omdat de taken van Europol en Eurojust waarschijnlijk met de tijd zullen evolueren.

De EDPS verzoekt de Commissie met klem om de taken waarvoor toegang van Europol en Eurojust gerechtvaardigd is, restrictief te omschrijven.

b. *Restrictie van gegevens*

Om „fishing expeditions" van Europol en Eurojust te vermijden, en om ervoor te zorgen dat zij alleen toegang krijgen tot de gegevens „die nodig zijn om hun taken te vervullen", heeft de GCA in haar advies van 27 september 2005 over de SIS II-voorstellen de suggestie gedaan om de toegang van Europol en Eurojust te beperken tot gegevens over personen wier naam al in hun bestanden staat. Aldus zou worden gewaarborgd dat alleen signaleringen die voor hen relevant zijn, kunnen worden geraadpleegd. De EDPS onderschrijft deze aanbeveling.

c. *Beveiligingsaspecten*

De EDPS is ingenomen met de verplichting om alle transacties in verband met Europol en Eurojust op te slaan, alsmede met het verbod om delen van het systeem te kopiëren of te downloaden.

Artikel 56 van het voorstel voor een besluit beoogt „één of twee" toegangspunten voor Europol en Eurojust. Hoe begrijpelijk het ook kan zijn dat een lidstaat vanwege de gedecentraliseerde structuur van zijn bevoegde autoriteiten meer dan één toegangspunt nodig heeft, de status en de activiteiten van Europol en Eurojust rechtvaardigen dit niet. Opgemerkt zij tevens dat, uit het oogpunt van de veiligheid, een verhoging van het aantal toegangspunten het gevaar van misbruik doet toenemen, en derhalve met consistentere elementen moet worden gerechtvaardigd. Bij gebreke van overtuigende argumenten stelt de EDPS derhalve voor om Europol en Eurojust slechts één toegangspunt te verlenen.

4.3. **Koppeling van signaleringen**

Artikel 26 van de verordening en artikel 46 van het besluit bepalen dat een lidstaat signaleringen overeenkomstig zijn nationale wetgeving kan koppelen, om twee of meer signaleringen met elkaar te verbinden.

Hoewel koppeling van signaleringen nuttig kan zijn voor controles (zo kan een aanhoudingsbevel voor een autodief worden gekoppeld aan een gestolen voertuig), gaat het hier om een typisch kenmerk van een politieel onderzoeksinstrument.

Koppeling van signaleringen kan een belangrijk effect hebben op de rechten van de betrokkene, omdat die niet langer wordt „beoordeeld" op basis van de hem betreffende gegevens, maar op basis van mogelijke associatie met andere personen. Personen wier gegevens gekoppeld zijn aan die van misdadigers of gezochte personen, zullen waarschijnlijk met meer wantrouwen worden bejegend dan andere. Koppeling van signaleringen komt bovendien neer op uitbreiding van de onderzoeksbevoegdheden van het SIS, omdat daardoor de registratie van vermeende bendes of netwerken mogelijk wordt (indien bijvoorbeeld gegevens over illegale immigranten worden gekoppeld aan gegevens over mensenhandelaars). Tenslotte heeft koppeling van signaleringen, aangezien daarop de nationale wetgeving van toepassing is, mogelijkerwijs tot gevolg dat een koppeling die in één lidstaat als illegaal wordt aangemerkt, door een andere lidstaat wel kan worden bewerkstelligd, en dat aldus „illegale" gegevens in het systeem worden opgenomen.

[1] Besluit 2005/211/JBZ van de Raad van 24 februari 2005 betreffende de invoering van enkele nieuwe functies in het Schengeninformatiesysteem, inclusief bij de bestrijding van terrorisme (PB L 68 van 15.3.2005, blz. 44).

In de conclusies van de Raad van 14 juni 2004 over de aan SIS II te stellen functie-eisen wordt gesteld dat elke koppeling duidelijk moet beantwoorden aan operationele behoeften, het evenredigheidsbeginsel moet eerbiedigen en moet berusten op een duidelijk omschreven verband. Bovendien mag koppeling geen afbreuk doen aan de toegangsrechten. Hoe het ook zij, koppeling van signaleringen moet, aangezien het om een verwerking gaat, in overeenstemming zijn met de nationale wetgeving ter uitvoering van Richtlijn 95/46/EG en/of Verdrag 108.

In de voorstellen wordt herhaald dat het bestaan van koppelingen geen afbreuk mag doen aan de toegangsrechten (anders zou toegang worden verleend tot gegevens waarvan de verwerking overeenkomstig de nationale wetgeving onwettig is, wat in strijd is met artikel 6 van de richtlijn).

De EDPS wijst op het belang van een strikte uitlegging van artikel 26 van het verordeningsvoorstel en van artikel 46 van het voorstel voor een besluit: dit kan worden gewaarborgd door duidelijk te stellen dat autoriteiten die geen toegang hebben tot bepaalde categorieën van gegevens, evenmin toegang mogen hebben tot koppelingen met die categorieën, en zelfs niet op de hoogte mogen zijn van het bestaan van deze koppelingen. Koppelingen mogen niet zichtbaar zijn wanneer er geen recht van toegang is tot de gekoppelde gegevens.

Bovendien zou de EDPS willen worden geraadpleegd over de technische maatregelen om een en ander te waarborgen.

4.4. **Signaleringen ter fine van weigering van toegang**

4.4.1. *Gronden voor opneming*

Het gebruik van „signaleringen van onderdanen van derde landen ter fine van weigering van toegang" (artikel 15 van de verordening) heeft een beduidende weerslag op de vrijheden van de betrokkene: een op grond van deze bepaling gesignaleerde persoon heeft gedurende verscheidene jaren geen toegang meer tot het Schengengebied. Het betreft tot dusverre de meest voorkomende signalering wat betreft het aantal gesignaleerde personen. Gezien de gevolgen van deze signaleringscategorie en het aantal betrokken personen, moet uiterst zorgvuldig te werk worden gegaan bij de invulling en de uitvoering ervan. Hoewel dat ook voor de andere signaleringscategorieën geldt, zal de EDPS een specifiek hoofdstuk wijden aan deze signaleringscategorie, omdat zij specifieke problemen doet rijzen in verband met de gronden voor opneming.

De nieuwe signalering ter fine van weigering van toegang houdt verbeteringen in ten opzichte van de huidige situatie, maar is ook niet volledig bevredigend, omdat zij goeddeels gebaseerd is op instrumenten die nog niet zijn aangenomen, of zelfs nog niet zijn ingediend.

De verbeteringen zijn gelegen in een preciezere omschrijving van de gronden voor opneming van gegevens. De huidige redactie van de Schengenuitvoeringsovereenkomst heeft geleid tot aanzienlijke verschillen tussen de lidstaten wat betreft het aantal op grond van artikel 96 SUO gesignaleerde personen. De GCA Schengen heeft een alomvattende studie [1] terzake verricht en aanbevolen dat „de beleidsmakers zouden moeten overwegen om de gronden voor opneming van signaleringen in de afzonderlijke Schengenstaten te harmoniseren".

Het voorgestelde artikel 15 is gedetailleerder, wat positief moet worden onthaald.

Bovendien bevat artikel 15, lid 2, een opsomming van gevallen waarin personen niet kunnen worden gesignaleerd, omdat ze, op grond van verschillende statussen, legaal op het grondgebied van een lidstaat verblijven. Hoewel dat al uit de huidige Schengenuitvoeringsovereenkomst kon worden afgeleid, heeft de praktijk aangetoond dat de toepassing van dit mechanisme onderhevig is aan variatie tussen de lidstaten. Verduidelijking is dan ook een positief element.

De bovengenoemde bepaling staat echter ook bloot aan serieuze kritiek, omdat zij voor een groot deel gebaseerd is op een nog niet aangenomen tekst, namelijk de richtlijn betreffende terugkeer.

Na de aanname van de SIS II-voorstellen heeft de Commissie (op 1 september 2005) een richtlijn ingediend over gemeenschappelijke normen en procedures in de lidstaten voor de terugkeer van onderdanen van derde landen die illegaal op hun grondgebied verblijven; zolang deze tekst evenwel niet definitief is, kan hij niet worden beschouwd als geldige grondslag voor de opneming van gegevens in een systeem. De richtlijn druist met name in tegen artikel 8 EVRM, omdat inmenging in de persoonlijke levenssfeer van personen gerechtvaardigd moet worden met — onder meer — een duidelijke en toegankelijke wetgeving.

De EDPS verzoekt de Commissie dan ook met klem deze bepaling in te trekken, dan wel op grond van de bestaande wetgeving zo te herformuleren dat de betrokkene kan vernemen welke maatregelen de autoriteiten precies jegens hem kunnen nemen.

4.4.2. *Toegang tot de in artikel 15 bedoelde signaleringen*

Artikel 18 bepaalt welke autoriteiten toegang hebben tot deze signaleringen, en voor welke doeleinden. In de leden 1 en 2 van artikel 18 wordt bepaald welke autoriteiten toegang hebben tot de op grond van de richtlijn betreffende terugkeer opgenomen signaleringen. Verwezen wordt naar de opmerkingen hierboven.

[1] Verslag van de gemeenschappelijke controleautoriteit van Schengen over een inspectie van het gebruik van de in artikel 96 bedoelde signaleringen in het Schengeninformatiesysteem, Brussel, 20 juni 2005.

Artikel 18, lid 3, van het verordeningsvoorstel verleent toegang aan de voor toekenning van de vluchtelingenstatus bevoegde autoriteiten uit hoofde van een richtlijn die zelfs nog niet is ingediend. Bij gebreke van een beschikbare tekst verwijst de EDPS naar de opmerkingen hierboven.

4.4.3. *Bewaartermijn van de in artikel 15 bedoelde signaleringen*

Volgens artikel 20 mag de signalering slechts worden bewaard gedurende de periode van weigering van toegang die is vastgesteld in de beslissing (tot verwijdering of terugkeer). Dit stemt overeen met de gegevensbeschermingsregels. Bovendien wordt de signalering na vijf jaar automatisch verwijderd, tenzij de lidstaat die de gegevens in SIS II heeft opgenomen, anders beslist.

Passend toezicht op nationaal niveau moet ervoor zorgen dat de bewaartermijn niet automatisch wordt verlengd wanneer dit niet gerechtvaardigd is, en dat de lidstaten de gegevens vóór het verstrijken van de termijn van vijf jaar verwijderen, indien de periode van weigering van toegang korter is.

4.5. **Bewaartermijnen**

Hoewel het beginsel van bewaring hetzelfde blijft (als algemene regel geldt dat een signalering uit SIS II moet worden verwijderd zodra de in de signalering gevraagde maatregel is genomen), vloeit uit de voorstellen voort dat de bewaartermijn voor signaleringen in het algemeen is verlengd.

In de Schengenuitvoeringsovereenkomst is bepaald dat uiterlijk drie jaar (of één jaar, in het geval van ter fine van onopvallende controle opgenomen gegevens) na de opneming van de gegevens wordt getoetst of verdere opslag nodig is. De nieuwe voorstellen voorzien in automatische verwijdering (met de mogelijkheid van verzet van de signalerende lidstaat) na 5 jaar voor immigratiegegevens, na 10 jaar voor gegevens inzake aanhouding, vermiste personen en personen die in het kader van een gerechtelijke procedure worden gezocht, en na 3 jaar voor personen die moeten worden onderworpen aan onopvallende controle.

Ofschoon de lidstaten de gegevens in beginsel moeten verwijderen wanneer het doel van de signalering is verwezenlijkt, wordt de maximale bewaartermijn aanzienlijk verlengd (in de meeste gevallen is die drie keer zo lang), zonder enige motivering van de Commissie. Wat de immigratiegegevens betreft, kan men alleen maar gissen dat de termijn van 5 jaar gekoppeld is aan de periode van weigering van toegang die in de ontwerp-richtlijn betreffende terugkeer wordt voorgesteld. In alle andere gevallen is niet in te zien waarom de termijn is verlengd.

Signalering in het SIS kan aanzienlijke gevolgen met zich mee brengen voor het leven van de betrokkenen. Dat is met name zorgwekkend in het geval van signalering van personen ter fine van onopvallende of gerichte controle, omdat deze signaleringen op basis van vermoedens kunnen worden opgenomen.

De EDPS wil een gegronde reden voor de verlenging van de bewaartermijnen. Indien hiervoor geen overtuigende rechtvaardiging kan worden gegeven, stelt hij voor deze termijnen tot hun huidige duur te herleiden, met name in het geval van signaleringen ter fine van onopvallende of gerichte controle.

4.6. **Toegang van de autoriteiten die belast zijn met de afgifte van voertuigkentekenbewijzen**

Het belangrijkste vraagstuk houdt verband met de keuze van een meer dan twijfelachtige rechtsgrondslag. De Commissie slaagt er niet in de EDPS te overtuigen van het gebruik van een rechtsgrondslag van de eerste pijler in verband met „vervoer" voor een maatregel die ertoe strekt bestuurlijke autoriteiten toegang tot het SIS te verlenen met het oog op de preventie en de bestrijding van criminaliteit (smokkel van gestolen voertuigen). De noodzaak van een gegronde reden en een solide rechtsgrondslag voor het verlenen van toegang tot SIS II wordt uiteengezet in punt 4.2.2 van dit advies.

De EDPS verwijst naar de opmerkingen vervat in het advies van de GCA Schengen over de voorgestelde rechtsgrondslag voor SIS II. Met name het voorstel van de GCA Schengen om het voorstel voor een besluit te wijzigen teneinde er deze toegang in op te nemen, verdient aanbeveling.

5. ROL VAN DE COMMISSIE EN DE LIDSTATEN

Een duidelijke omschrijving en toewijzing van verantwoordelijkheden in het kader van SIS II is van het allergrootste belang, niet alleen voor de goede werking van het systeem, maar ook uit het oogpunt van toezicht. De bevoegdheidsverdeling op het gebied van het toezicht vloeit voort uit de omschrijving van de verantwoordelijkheden; absolute duidelijkheid is dan ook een noodzaak.

5.1. **Rol van de Commissie**

De EDPS is ingenomen met hoofdstuk III van beide voorstellen, waarin de rol en de verantwoordelijkheden van de Commissie in het kader van SIS II (als een rol van „operationeel beheer") worden omschreven. Die verduidelijking blijft in het VIS-voorstel achterwege. De rol van de Commissie wordt evenwel niet uitsluitend in hoofdstuk III bepaald. Zoals reeds besproken in hoofdstuk 9 van dit advies, is de Commissie via de comitologieprocedure tevens betrokken bij de uitvoering en het beheer van het systeem.

Wat gegevensbescherming betreft, heeft de Commissie een rol die al in het kader van het VIS en Eurodac is erkend, namelijk de rol van verantwoordelijke voor het operationele beheer. Samen met haar belangrijke rol op het vlak van de ontwikkeling en het onderhoud van het systeem, moet deze rol worden beschouwd als de rol van een toezichthouder *sui generis*. Zoals vermeld in het advies van de EDPS over het VIS, houdt dit veel meer in dan de taak van een gegevensverwerker, maar is het tegelijk beperkter dan de taak van een normale toezichthouder, doordat de Commissie geen toegang heeft tot de in het SIS II verwerkte gegevens.

Aangezien SIS II gebaseerd zal zijn op complexe systemen, waarvan sommige berusten op nieuwe technologieën, dringt de EDPS aan op een grotere verantwoordelijkheid van de Commissie voor het up-to-date houden van de systemen door de beste beschikbare technologie in verband met beveiliging en gegevensbescherming toe te passen.

In artikel 12 van de voorstellen dient derhalve te worden toegevoegd dat de Commissie regelmatig voorstellen moet doen voor de implementatie van nieuwe technologieën die beantwoorden aan de jongste stand van de techniek op dit gebied, de gegevensbescherming en veiligheidsniveaus zullen verbeteren en de taken van de nationale autoriteiten die toegang hebben tot deze gegevens, zullen vergemakkelijken.

5.2. **Rol van de lidstaten**

De situatie van de lidstaten is niet echt duidelijk, omdat moeilijk uit te maken valt welke autoriteiten zullen fungeren als toezichthouder.

In de voorstellen wordt een omschrijving gegeven van de rol van de nationale SIS II-instantie (zorgen voor toegang van de bevoegde autoriteiten tot SIS II) en van de Sirene-autoriteit (zorgen voor de uitwisseling van alle aanvullende informatie). De lidstaten moeten tevens zorgen voor de werking en de beveiliging van hun „NS" („Nationaal Systeem"). Het is niet duidelijk of laatstgenoemde verantwoordelijkheid door één van de bovengenoemde autoriteiten moet worden gedragen. In ieder geval dient een en ander te worden verduidelijkt.

Wat gegevensbescherming betreft, moeten de Commissie en de lidstaten als één toezichthouder worden beschouwd, zij het elk met specifieke verantwoordelijkheden. Erkenning van deze complementaire taken is de enige weg naar volledig toezicht op alle SIS II-activiteiten.

6. **RECHTEN VAN DE BETROKKENE**

6.1. **Informatie**

6.1.1. *Verordeningsvoorstel*

Artikel 28 van het verordeningsvoorstel voorziet in het recht van informatie van de betrokkene, en is voornamelijk gebaseerd op artikel 10 van Richtlijn 95/46. Dit is een wijziging ten goede, want de Schengenuitvoeringsovereenkomst voorziet niet uitdrukkelijk in een recht van informatie. De volgende punten zijn evenwel voor verbetering vatbaar.

Er moet informatie worden toegevoegd aan de lijst: dat zou bijdragen tot een eerlijke behandeling van de betrokkene ([1]). Die informatie heeft betrekking op de bewaartermijn van de gegevens, het bestaan van het recht om een besluit tot opneming van een signalering te laten toetsen of daartegen beroep in te stellen (in sommige gevallen, zie artikel 15, lid 3, van het verordeningsvoorstel), de mogelijkheid om bijgestaan te worden door de gegevensbeschermingsautoriteit, en het bestaan van rechtsmiddelen.

Het verordeningsvoorstel bevat geen aanwijzingen omtrent het tijdstip waarop de informatie moet worden verstrekt. Daardoor zou het voor de betrokkene onmogelijk kunnen zijn om zijn rechten te doen gelden Om deze rechten te kunnen doen gelden, dient de verordening te voorzien in een tijdstip waarop de informatie moet worden verstrekt, een tijdstip dat afhankelijk is van de signalerende autoriteit.

Een praktische oplossing zou erin bestaan informatie over de signalering op te nemen in het besluit dat aan de signalering ten grondslag ligt: een rechterlijke of administratieve beslissing die wordt gerechtvaardigd door een gevaar voor de openbare orde (…), een terugkeerbesluit of een uitzettingsbevel gepaard gaand met een verbod om het land opnieuw binnen te komen. Bovenstaande informatie moet worden toegevoegd aan artikel 28 van de verordening.

6.1.2. *Voorgestelde besluit*

In artikel 50 van het besluit wordt bepaald dat informatie wordt verstrekt op verzoek van de persoon van wie gegevens worden verwerkt (de betrokkene), en worden de mogelijke gronden voor het weigeren van informatie genoemd. Gezien de aard van de gegevens en de context waarin deze worden verwerkt, valt het natuurlijk te begrijpen dat aan dit recht beperkingen worden gesteld.

Het recht van informatie mag echter niet afhankelijk worden gemaakt van een verzoek van de betrokkene (eigenlijk zou een verzoek om toegang eerder zo moeten worden gedefinieerd). Er kan worden verondersteld dat het gerechtvaardigd is om informatie te „verzoeken" in de gevallen waarin de betrokkene niet kan worden geïnformeerd omdat niet bekend is waar hij zich bevindt.

Dit zou beter worden aangepakt door een uitzondering op het recht van informatie toe te voegen in gevallen waarin het verstrekken van informatie onmogelijk is of een buitensporige inspanning vergt. Artikel 50 van het besluit moet dienovereenkomstig worden gewijzigd.

([1]) Zie het advies van de EDPS over het visuminformatiesysteem, punt 3.10.1.

Deze oplossing zou ook stroken met de toepassing van het ontwerp-kaderbesluit over gegevensbescherming in het kader van de derde pijler.

6.2. **Toegang**

Het is positief te noemen dat zowel in het verordeningsvoorstel als in het voorgestelde besluit termijnen worden opgelegd voor het beantwoorden van verzoeken om toegang. Aangezien de procedure voor de uitoefening van het recht van toegang op nationaal niveau is gedefinieerd, kan echter de vraag worden gesteld hoe de termijnen die in deze voorstellen worden opgelegd, in de bestaande procedures kunnen worden ingepast, met name indien in bepaalde lidstaten kortere termijnen van toepassing zijn voor de beantwoording van een verzoek om toegang. Er moet duidelijk worden gemaakt dat de termijnen die het meest in het voordeel van de betrokkene zijn, moeten worden toegepast.

6.2.1. *Verordeningsvoorstel*

Opgemerkt zij dat de huidige beperkingen op het recht van toegang in de Schengenovereenkomst („wordt geweigerd, wanneer dat voor de uitoefening van een rechtmatige taak in verband met de in SIS II opgenomen gegevens of ter bescherming van de rechten en vrijheden van de betrokken persoon of van derden onontbeerlijk is") niet in het verordeningsvoorstel zijn opgenomen.

Dit is echter wellicht het gevolg van de toepasselijkheid van Richtlijn 95/46/EG, die (in artikel 13) in de mogelijkheid van uitzonderingen in de nationale wetgeving voorziet. In elk geval moet worden aangetekend dat het gebruik van artikel 13 in de nationale wetgeving met het oog op het beperken van het recht van toegang steeds in overeenstemming moet zijn met artikel 8 EVRM en slechts in een beperkt aantal gevallen kan worden toegepast.

6.2.2. *Voorgestelde besluit*

In het voorgestelde besluit wordt de beperking van het recht van toegang uit de Schengenovereenkomst overgenomen. Het voorstel voor het kaderbesluit bevat in essentie dezelfde beperkingen van het recht van toegang; op dit punt zal de aanneming van dit instrument bijgevolg geen significant verschil uitmaken.

Aangezien de toegang tot wetshandhavingsgegevens in verschillende lidstaten „indirect" is (dit betekent dat deze toegang wordt uitgeoefend via de nationale gegevensbeschermingsautoriteit), zou moeten worden voorzien in de verplichting dat de gegevensbeschermingsautoriteiten actief samenwerken bij de uitoefening van het recht van toegang.

6.3. **Recht om de beslissing tot opneming van een signalering te laten toetsen of daartegen beroep in te stellen**

In artikel 15, lid 3, van de verordening is het recht opgenomen om een beslissing om een signalering op te nemen die door een administratieve autoriteit is vastgesteld, te laten toetsen door of daartegen beroep in te stellen bij een justitiële autoriteit. In vergelijking met de huidige Schengenovereenkomst is dit een welkome toevoeging.

Hiermee wordt kracht bijgezet aan de noodzaak om de betrokkene tijdig volledig te informeren, zoals gesteld in punt 6.1 hierboven: zonder deze informatie zou dit nieuwe recht inhoudsloos blijven.

6.4. **Rechtsmiddelen**

In artikel 30 van het verordeningsvoorstel alsmede in artikel 52 van het voorgestelde besluit wordt bepaald dat eenieder het recht heeft op het grondgebied van een lidstaat een rechtsvordering in te stellen of een klacht in te dienen indien hem het recht is ontzegd om toegang te krijgen tot de hem betreffende gegevens of om deze gegevens te laten rechtzetten of verwijderen of om informatie of schadevergoeding te krijgen.

De gekozen formulering („Eenieder heeft het recht op het grondgebied van een lidstaat…") suggereert dat de eiser fysiek op het grondgebied aanwezig moet zijn om een rechtsvordering te kunnen instellen. Deze territoriale beperking is niet gerechtvaardigd en kan afbreuk doen aan de efficiëntie van het recht op rechtsmiddelen, aangezien het voor de hand ligt dat in vele gevallen de eiser juist een rechtsvordering zal instellen omdat hem geen toegang tot het Schengengrondgebied wordt verleend. Wat het verordeningsvoorstel betreft, moet, aangezien de richtlijn de *lex generalis* is, rekening worden gehouden met artikel 22 van de richtlijn; daarin wordt bepaald dat „eenieder" het recht op rechtsmiddelen heeft, ongeacht zijn of haar verblijfplaats. Het voorgestelde kaderbesluit bevat evenmin een territoriale beperking. De EDPS stelt voor om de territoriale beperking in artikel 30 en in artikel 52 te schrappen.

7. **TOEZICHT**

7.1. **Inleiding: gedeelde verantwoordelijkheden**

In de voorstellen wordt de toezichthoudende taak over de nationale controleautoriteiten ([1]) en de EDPS verdeeld, elk voor wat hun eigen bevoegdheden betreft. Dit strookt met de wijze waarop in de voorstellen de toepasselijke wetgeving en de verantwoordelijkheden voor de werking en het gebruik van het SIS II worden benaderd, en met de noodzaak van een doeltreffend toezicht.

De EDPS juicht daarom deze benadering in artikel 31 van het verordeningsvoorstel en in artikel 53 van het voorgestelde besluit toe. Voor een beter begrip en ter verduidelijking van de respectieve taken stelt de EDPS echter voor om elk artikel op te splitsen in verschillende leden, die elk gewijd zijn aan een bepaald niveau van toezicht, naar analogie van het VIS-voorstel.

([1]) De controleautoriteiten van Europol en Eurojust spelen ook een rol, zij het in mindere mate.

7.2. **Toezicht door de nationale gegevensbeschermingsautoriteiten**

Op grond van artikel 31 van het verordeningsvoorstel en artikel 53 van het voorgestelde besluit moet elke lidstaat ervoor zorgen dat een onafhankelijke autoriteit toezicht houdt op de rechtmatigheid van de verwerking van SIS II-persoonsgegevens.

In artikel 53 van het voorgestelde besluit wordt daaraan toegevoegd dat eenieder het recht heeft de controleautoriteiten te verzoeken de rechtmatigheid van de verwerking van de hem betreffende gegevens te toetsen. Een vergelijkbare bepaling is niet opgenomen in het verordeningsvoorstel, aangezien de richtlijn van toepassing is als *lex generalis*. Er moet derhalve van worden uitgegaan dat de nationale gegevensbeschermingsautoriteiten met betrekking tot het SIS II alle bevoegdheden kunnen uitoefenen die hen in artikel 28 van Richtlijn 95/46/EG worden toegedeeld, met inbegrip van het toezicht op de rechtmatigheid van de gegevensverwerking. Artikel 31, lid 1, van de verordening vormt een verduidelijking van hun taken, maar kan geen beperking van deze bevoegdheden inhouden. De erkenning van deze bevoegdheden moet in de tekst van het verordeningsvoorstel worden verduidelijkt.

In vergelijking met het voorgestelde besluit worden in het verordeningsvoorstel uitvoeriger taken van de nationale controleautoriteiten erkend, omdat de *lex generalis* anders is. Een situatie waarin de controleautoriteiten verschillende taken en bevoegdheden hebben al naargelang de categorie gegevens die worden verwerkt, is echter niet deugelijk en valt in de praktijk zeer moeilijk te beheren. Een dergelijke situatie moet derhalve worden voorkomen, hetzij door deze autoriteiten dezelfde bevoegdheden toe te delen in de tekst van het voorgestelde besluit, hetzij door naar een andere *lex generalis* te verwijzen (namelijk het kaderbesluit over gegevensbescherming in het kader van de derde pijler) waarin de gegevensbeschermingsautoriteiten meer bevoegdheden wordt gegeven.

7.3. **Toezicht door de EDPS**

De EDPS ziet erop toe dat de verwerking van gegevens door de Commissie gebeurt overeenkomstig de betreffende wetgevingsvoorstellen. De EDPS moet tevens al zijn bevoegdheden op grond van Verordening (EG) nr. 45/2001 kunnen uitoefenen, met dien verstande evenwel dat de bevoegdheden van de Commissie met betrekking tot de gegevens zelf beperkt zijn.

Hieraan moet worden toegevoegd dat, overeenkomstig artikel 46, punt f), van Verordening (EG) nr. 45/2001, de EDPS „met de nationale toezichthoudende autoriteiten samenwerkt, voorzover dat voor de uitoefening van hun onderscheiden taken nodig is". De samenwerking met de lidstaten bij het toezicht op het SIS II vloeit niet alleen voort uit de nieuwe wetgevingsvoorstellen, maar ook uit Verordening (EG) nr. 45/2001.

7.4. **Gemeenschappelijk toezicht**

In de voorstellen wordt ook erkend dat de controleactiviteiten van de verschillende betrokken autoriteiten moeten worden gecoördineerd. In artikel 31 van het verordeningsvoorstel en in artikel 53 van het voorgestelde besluit wordt het volgende bepaald: „De nationale controleautoriteiten en de Europese toezichthouder voor gegevensbescherming werken actief samen. De Europese toezichthouder voor gegevensbescherming belegt daartoe minstens eenmaal per jaar een vergadering".

De EDPS is verheugd over dit voorstel, dat de noodzakelijke elementen in zich draagt om te zorgen voor samenwerking — die inderdaad van cruciaal belang is — tussen de autoriteiten die op nationaal en op Europees niveau met toezicht zijn belast. Beklemtoond zij dat in de voorstellen weliswaar wordt bepaald dat ten minste eenmaal per jaar een vergadering plaatsvindt, maar dit moet als een minimum worden beschouwd.

Deze bepalingen (artikel 31 van het verordeningsvoorstel en artikel 53 van het voorgestelde besluit) behoeven echter verduidelijking met betrekking tot de inhoud van die coördinatie. De bestaande GCA is bevoegd om moeilijkheden bij de uitlegging of toepassing van de Schengenovereenkomst te behandelen, zich te buigen over problemen die zich kunnen voordoen bij de uitoefening van onafhankelijk toezicht of van het recht van toegang, en om geharmoniseerde voorstellen te doen voor gemeenschappelijke probleemoplossing.

De nieuwe voorstellen mogen de huidige reikwijdte van het gemeenschappelijke toezicht niet afzwakken. Het is duidelijk dat de gegevensbeschermingsautoriteiten met betrekking tot het SIS II alle toezichthoudende bevoegdheden kunnen uitoefenen die hen op grond van de richtlijn zijn toegedeeld, en dat de samenwerking tussen die autoriteiten tal van aspecten van het toezicht op het SIS II kan omvatten, daaronder begrepen de taken van de bestaande GCA als bedoeld in artikel 115 van de Schengenovereenkomst.

Om dit volkomen duidelijk te maken, zou dit echter in de voorstellen nog eens uitdrukkelijk moeten worden opgenomen.

8. **BEVEILIGING**

Het beheer en de inachtneming van een optimaal beveiligingsniveau voor het SIS II is een basisvereiste voor een passende bescherming van de in het gegevensbestand opgenomen persoonsgegevens. Om dit beschermingsniveau te kunnen halen, moeten specifieke garanties worden ingebouwd om het hoofd te kunnen bieden aan de potentiële risico's die gepaard gaan met de systeeminfrastructuur en de betrokken personen. Dit punt wordt thans in verschillende delen van het voorstel behandeld en behoeft verbetering.

De artikelen 10 en 13 van het voorstel bevatten verschillende maatregelen voor de beveiliging van de gegevens en specificeren welke soorten misbruiken moeten worden voorkomen. De EDPS juicht toe dat in deze artikelen bepalingen betreffende systematische (interne) controle van de beveiligingsmaatregelen zijn opgenomen.

Artikel 59 van het voorgestelde besluit en artikel 34 van het verordeningsvoorstel, die bepalingen inzake toezicht en evaluatie bevatten, mogen echter niet alleen betrekking hebben op de resultaten, de kosteneffectiviteit en de kwaliteit van de dienstverlening, maar moeten ook gaan over de mate waarin aan de wettelijke voorschriften wordt voldaan, met name op het gebied van gegevensbescherming. De EDPS beveelt derhalve aan de reikwijdte van deze artikelen uit te breiden tot toezicht op en rapportering over de rechtmatigheid van de verwerking.

Als aanvulling op artikel 10, lid 1, punt f), of artikel 18 van het voorgestelde besluit en artikel 17 van het verordeningsvoorstel betreffende de naar behoren gemachtigde personeelsleden die toegang hebben tot de gegevens, dient ook te worden toegevoegd dat de lidstaten (alsmede Europol en Eurojust) ervoor moeten zorgen dat er precieze gebruikersprofielen voorhanden zijn (die ten behoeve van controle ter beschikking van de nationale controleautoriteiten moeten worden gehouden). Naast deze gebruikersprofielen moet een volledige lijst van gebruikersidentiteiten worden opgesteld en permanent door de lidstaten worden bijgewerkt. Dit geldt *mutatis mutandis* ook voor de Commissie.

Deze beveiligingsmaatregelen worden aangevuld met organisatorische en controlegaranties. In artikel 14 van het voorstel staat beschreven onder welke voorwaarden en voor welke doeleinden een register van alle gegevensverwerkingshandelingen moet worden gehouden. Deze registers moeten worden opgeslagen om de gegevensbescherming te kunnen controleren en de gegevensbeveiliging te kunnen garanderen, alsook om de regelmatige interne controle van het SIS II op grond van artikel 10 te consolideren. De interne-controleverslagen zullen ertoe bijdragen dat de controleautoriteiten hun taken doeltreffend kunnen uitvoeren, doordat zij de zwakste punten zullen kunnen blootleggen en zich tijdens hun eigen controle daarop zullen kunnen toeleggen.

Zoals eerder gesteld in dit advies, moet uitvoerig worden gerechtvaardigd waarom er meer toegangspunten tot het systeem zijn, aangezien het gevaar van misbruik daardoor groter wordt. Op grond van artikel 4, lid 1, punt b), van de voorstellen moet derhalve worden verlangd dat concreet wordt aangetoond waarom een tweede toegangspunt nodig is.

In de voorstellen wordt niet duidelijk uitgelegd waarom er nationale kopieën van het centrale systeem nodig zijn, hetgeen aanleiding geeft tot grote bezorgdheid over het algemene risico- en veiligheidsniveau van het systeem, bijvoorbeeld:

— de toename van het aantal kopieën verhoogt het risico van misbruik (met name gelet op de aanwezigheid van nieuwe gegevens, zoals biometrische gegevens);

— er is niet duidelijk gedefinieerd welke gegevens worden gekopieerd;

— de in artikel 9 opgenomen eisen inzake accuraatheid, kwaliteit en beschikbaarheid vormen een grote technische uitdaging en jagen de kosten bijgevolg de hoogte in, in verband met de nieuwste stand van de beschikbare technologie;

— het toezicht op deze kopieën door de nationale autoriteiten zal extra personele en financiële middelen vergen, die misschien niet altijd beschikbaar zijn.

Gezien de daaraan verbonden risico's is de EDPS niet overtuigd van de noodzaak (gelet op de beschikbare technologie) of de meerwaarde van het gebruik van nationale kopieën. Hij beveelt aan om af te zien van de mogelijkheid dat de lidstaten nationale kopieën gebruiken.

Indien er nationale kopieën worden ontwikkeld, dan herinnert de EDPS eraan dat het gebruik van dergelijke nationale kopieën onderworpen moet zijn aan een strikt beginsel van doelbeperking. Voorts mag een nationale kopie nooit op een andere manier worden aangezocht dan de centrale gegevensbank.

De rechtmatigheid van de verwerking van persoonsgegevens berust op de strikte naleving van gegevensbeveiliging en gegevensintegriteit. De EDPS zal zorgen voor efficiënte controle; hij kan niet alleen de beveiliging van de gegevens, maar ook, door analyse van de beschikbare registers, de integriteit ervan controleren. Derhalve moet aan artikel 14, lid 6, „gegevensintegriteit" worden toegevoegd.

9. **COMITOLOGIE**

De voorstellen voorzien in comitologieprocedures voor de verschillende gevallen waarin technische besluiten moeten worden genomen ten behoeve van de uitvoering of het beheer van het SIS II. Zoals om vergelijkbare redenen in het advies over het VIS is gesteld, zullen deze besluiten een grote stempel drukken op de eigenlijke toepassing van het beginsel van doelbinding en proportionaliteit.

De EDPS adviseert dat beslissingen die ingrijpende gevolgen hebben voor de gegevensbescherming, zoals toegang tot en invoering van gegevens, uitwisseling van aanvullende informatie, kwaliteit van gegevens en verenigbaarheid van signaleringen, technische overeenstemming van nationale kopieën, enz. in de vorm van een verordening of een besluit worden genomen, bij voorkeur in het kader van de medebeslissingsprocedure ([1]).

([1]) Zie hierover ook punt 3.12 van het advies van de EDPS over het Visuminformatiesysteem, en punt 60 van het advies van de EDPS van 26 september 2005 over het voorstel voor een richtlijn betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten.

Voor alle andere gevallen die gevolgen hebben voor de gegevensbescherming, moet de EDPS in de mogelijkheid worden gesteld advies uit te brengen over de door de betreffende comités gemaakte keuzes.

De adviserende rol van de EDPS moet worden opgenomen in de artikelen 60 en 61 van het besluit en in artikel 35 van de verordening.

Wat het meer specifieke geval van de technische voorschriften voor koppelingen tussen signaleringen betreft (artikel 26 van de verordening en artikel 46 van het besluit), moet worden verduidelijkt dat er een andere comitologieprocedure (adviesprocedure voor het besluit, en regelgevingsprocedure voor de verordening) vereist is.

10. **INTEROPERABILITEIT**

Bij ontstentenis van de mededeling van de Commissie over de interoperabiliteit van nieuwe EU-systemen, valt de meerwaarde van de beoogde, maar nog niet gedefinieerde synergieën moeilijk naar behoren te evalueren.

In dit verband verwijst de EDPS tevens 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 verwijst hij 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).

In zijn advies over het Visuminformatiesysteem heeft de EDPS reeds verklaard dat interoperabiliteit een kritieke en essentiële voorwaarde is voor de doeltreffendheid van grootschalige IT-systemen zoals SIS II. 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 beoogde handhaving van een hoog niveau van veiligheid in een ruimte zonder controles aan de binnengrenzen tussen de lidstaten 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 signaleringen die door de autoriteiten van de ene lidstaat worden toegestuurd moeten interoperabel zijn met de signaleringen die de autoriteiten van een andere lidstaat toesturen.

  — 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. Voorzover uit de voorstellen valt op te maken, blijkt bijvoorbeeld dat er in de eerste jaren van het SIS II geen automatisch vingerafdrukkenidentificatiesysteem (AFIS) voorhanden zal zijn; er is alleen sprake van een toekomstige biometrische zoekmachine. Indien een scenario wordt overwogen waarin een AFIS van een ander EU-systeem wordt gebruikt, moet dit duidelijk worden gedocumenteerd, met de nodige garanties die voor dergelijke synergieën vereist zijn.

De EDPS wenst nogmaals te benadrukken dat de invoering van interoperabiliteit tussen systemen 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.

11. **SAMENVATTING VAN DE CONCLUSIES**

11.1. **Algemene punten**

1. De EDPS is verheugd over de diverse positieve aspecten van deze voorstellen, die op een aantal punten een verbetering ten opzichte van de huidige situatie inhouden. Hij erkent dat de bepalingen inzake gegevensbescherming over het algemeen met de grootste zorg zijn opgesteld.

2. De EDPS beklemtoont dat het nieuwe rechtskader, hoe complex ook,

   — moet zorgen voor een hoog niveau van gegevensbescherming;

   — voorspelbaar moet zijn voor de burgers en voor de autoriteiten die gegevens uitwisselen;

   — in zijn toepassing moet stroken met verschillende contexten (eerste of derde pijler).

3. Voorts moet de toevoeging van nieuwe elementen in het SIS II, waardoor de mogelijke gevolgen van het systeem voor de individuele levenssfeer toenemen, gepaard gaan met stringentere garanties, zoals beschreven in dit advies. Meer bepaald het volgende:

— er kan aan nieuwe instanties geen toegang tot het SIS II worden verleend zonder dat dit zeer uitvoerig wordt gerechtvaardigd. Bovendien moet de toegang zoveel mogelijk worden beperkt, zowel wat de toegankelijke gegevens als wat de gemachtigde personen betreft.

— een koppeling tussen signaleringen mag nooit, zelfs niet indirect, leiden tot een wijziging van de toegangsrechten.

— niet-aangenomen wetgeving kan niet worden beschouwd als geldige grond voor het opnemen van gegevens in het SIS II (signaleringen met het oog op weigering van toegang).

— de rechtsgrondslag voor de toegang van de instanties die belast zijn met de afgifte van kentekenbewijzen van voertuigen moet opnieuw worden bekeken, aangezien deze hoofdzakelijk voor criminaliteitsbestrijding is bedoeld.

— de EDPS erkent dat het gebruik van biometrische gegevens de prestaties van het systeem kan verbeteren en slachtoffers van identiteitsmisbruik kan helpen. Er lijkt echter niet voldoende te zijn nagedacht over de gevolgen van de opneming daarvan, en de betrouwbaarheid van deze gegevens lijkt te zijn overschat.

11.2. **Specifieke opmerkingen**

1. Het verheugt de EDPS dat de Commissie erkent dat Verordening (EG) nr. 45/2001 van toepassing is op alle gegevensverwerkingsactiviteiten van de Commissie in het kader van het SIS II, want dit zal mede zorgen voor een samenhangende en eenvormige toepassing van de voorschriften ter bescherming van de fundamentele rechten en vrijheden van het individu in verband met de verwerking van persoonsgegevens.

2. Teneinde een strikte beperking van het doel op nationaal niveau te garanderen, stelt de EDPS voor om in de SIS II-voorstellen (namelijk in artikel 21 van de voorgestelde verordening en in artikel 40 van het voorgestelde besluit) een bepaling op te nemen in de trant van artikel 102, lid 4, van de Schengenuitvoeringsovereenkomst, ter beperking van de mogelijkheid voor de lidstaten om te voorzien in gebruik van gegevens waar de SIS II-teksten niet in voorzien.

3. De volgende strikte voorwaarden moeten van toepassing zijn wanneer instanties toegang wordt verleend tot het SIS II:

— de toegang moet verenigbaar zijn met het algemene doel van het SIS II, en in overeenstemming zijn met de rechtsgrondslag ervan.

— de noodzaak van de toegang tot de in het SIS II opgenomen gegevens moet aangetoond zijn.

— het beoogde gebruik van de gegevens moet uitdrukkelijk en restrictief worden omschreven.

— de voorwaarden voor toegang moeten welomschreven en restrictief zijn. Meer in het bijzonder moet er een bijgewerkte lijst voorhanden zijn van personen die toegang hebben tot het SIS II, ook voor Europol en Eurojust.

— het feit dat deze autoriteiten toegang tot SIS II-gegevens krijgen, kan nimmer een grond zijn voor opneming of handhaving in het systeem van gegevens die niet dienstig zijn voor de specifieke signalering waarop zij betrekking hebben.

— de bewaartermijn van de gegevens mag niet worden verlengd wanneer dat niet nodig is voor het doel waarvoor de gegevens zijn opgenomen.

4. Wat de specifieke gevallen van Europol en Eurojust betreft, verzoekt de EDPS de Commissie met klem om de taken waarvoor toegang gerechtvaardigd is, restrictief te omschrijven. De toegang van Europol en Eurojust moet bovendien worden beperkt tot gegevens over personen van wie de naam reeds in de Europol- of Eurojust-bestanden voorkomt. Verder wordt voorgesteld om Europol en Eurojust slechts één toegangspunt ter beschikking te stellen.

5. Wat signaleringen met het oog op weigering van toegang betreft, moeten bepalingen die op nog niet aangenomen wetgeving zijn gebaseerd, worden ingetrokken of zodanig worden geherformuleerd — op basis van bestaande wetgeving — dat personen kunnen weten welke maatregelen de autoriteiten precies tegen hen kunnen nemen.

6. De bewaartermijnen van de gegevens zijn verlengd zonder dat daarvoor gegronde redenen zijn aangevoerd. Indien hiervoor geen overtuigende rechtvaardiging kan worden gegeven, moeten deze termijnen tot hun huidige duur worden teruggebracht, met name in het geval van signaleringen met het oog op onopvallende of gerichte controles.

7. De rol van de Commissie wordt beschreven als de rol van verantwoordelijke voor het operationele beheer. Samen met haar belangrijke rol op het vlak van de ontwikkeling en het onderhoud van het systeem, moet deze rol worden beschouwd als toezichthouder *sui generis*. Dit houdt veel meer in dan de taak van een gegevensverwerker, maar is tegelijk beperkter dan de taak van een normale toezichthouder, doordat de Commissie geen toegang heeft tot de in het SIS II verwerkte gegevens.

   In het verlengde van deze rol moet in artikel 12 van de beide voorstellen worden toegevoegd dat de Commissie regelmatig voorstellen moet doen voor de implementatie van nieuwe technologieën die beantwoorden aan de jongste stand van de techniek op dit gebied en de gegevensbescherming en veiligheidsniveaus zullen verbeteren.

8. Wat de rol van de lidstaten betreft, moet worden verduidelijkt welke autoriteiten controle zullen uitoefenen.

9. Wat betreft het informeren van de persoon wiens gegevens worden verwerkt:

   — moet in de voorgestelde verordening de volgende informatie aan de lijst worden toegevoegd: de bewaartermijn van de gegevens, het bestaan van het recht om een beslissing om een signalering op te nemen, te laten toetsen of daartegen beroep in te stellen, de mogelijkheid om bijgestaan te worden door de gegevensbeschermingsautoriteit, en het bestaan van rechtsmiddelen.

     Wat het tijdstip betreft waarop deze informatie wordt verstrekt, moet de verplichting worden opgenomen dat de informatie over de signalering in de eerste plaats moet worden verstrekt in het besluit waarop de signalering is gebaseerd.

   — moet in het voorgestelde besluit artikel 50 zodanig worden gewijzigd dat het recht van informatie niet langer afhankelijk is van een verzoek van de betrokkene.

10. Wat de termijnen voor de beantwoording van een verzoek om toegang betreft, is het verheugend dat in de voorstellen termijnen worden opgelegd. Wanneer in de nationale wetgeving eveneens termijnen worden opgelegd, moet duidelijk worden gemaakt dat de termijnen die het meest in het voordeel van de betrokkene zijn, toegepast moeten worden.

    Verder zou het dienstig zijn om de gegevensbeschermingsautoriteiten te verplichten tot actieve samenwerking bij de uitoefening van het recht van toegang.

11. Wat het recht op rechtsmiddelen betreft, stelt de EDPS voor om de territoriale beperking in artikel 30 en in artikel 52 te schrappen.

12. Wat de bevoegdheden van de nationale gegevensbeschermingsautoriteiten betreft:

    — in de verordening: moet voor ogen worden gehouden dat zij, met betrekking tot het SIS II, alle bevoegdheden kunnen uitoefenen die hun op grond van artikel 28 van Richtlijn 95/46/EG zijn toegedeeld; dit moet in de tekst van het verordeningsvoorstel worden verduidelijkt.

    — wat het voorgestelde besluit betreft: moeten de toezichthoudende autoriteiten dezelfde bevoegdheden krijgen als in de verordening/richtlijn.

13. Wat de bevoegdheden van de EDPS betreft: de EDPS moet al zijn bevoegdheden op grond van Verordening (EG) nr. 45/2001 kunnen uitoefenen, evenwel rekening houdend met de beperkte bevoegdheden van de Commissie met betrekking tot de gegevens zelf.

14. Wat het gecoördineerde toezicht betreft: wordt in de voorstellen ook erkend dat de controleactiviteiten van de verschillende betrokken autoriteiten moeten worden gecoördineerd. De EDPS juicht toe dat de voorstellen de noodzakelijke elementen in zich dragen om te zorgen voor samenwerking tussen de autoriteiten die op nationaal en op Europees niveau met toezicht zijn belast. Deze bepalingen (artikel 31 van het verordeningsvoorstel en artikel 53 van het voorgestelde besluit) behoeven echter verduidelijking met betrekking tot de inhoud van die coördinatie.

15. De artikelen 10 en 13 van het voorstel bevatten verschillende gegevensbeveiligingsmaatregelen: de opneming van bepalingen over systematische (interne) controle van de beveiligingsmaatregelen wordt toegejuicht.

    — Artikel 59 van het voorgestelde besluit en artikel 34 van het verordeningsvoorstel, die bepalingen inzake toezicht en evaluatie bevatten, mogen echter niet alleen betrekking hebben op de resultaten, de kosteneffectiviteit en de kwaliteit van de dienstverlening, maar moeten ook gaan over de mate waarin aan de wettelijke voorschriften wordt voldaan, met name op het gebied van gegevensbescherming. Deze bepalingen moeten dienovereenkomstig worden gewijzigd.

    — Als aanvulling op artikel 10, lid 1, punt f), of artikel 18 van het voorgestelde besluit en artikel 17 van het verordeningsvoorstel dient te worden toegevoegd dat de lidstaten, Europol en Eurojust ervoor moeten zorgen dat precieze gebruikersprofielen voorhanden zijn (die ten behoeve van controle ter beschikking van de nationale controleautoriteiten moeten worden gehouden). Naast deze gebruikersprofielen moet een volledige lijst van gebruikersidentiteiten worden opgesteld en permanent door de lidstaten worden bijgewerkt. Dit geldt ook voor de Commissie.

    — De rechtmatigheid van de verwerking van persoonsgegevens berust op de strikte naleving van gegevensbeveiliging en gegevensintegriteit. De EDPS moet in staat worden gesteld om niet alleen de beveiliging, maar ook de integriteit van de gegevens — door analyse van de beschikbare registers — te controleren. Derhalve moet aan artikel 14, lid 6, „gegevensintegriteit" worden toegevoegd.

16. Het gebruik van nationale kopieën kan heel wat extra gevaren opleveren. De EDPS is niet overtuigd van de noodzaak (gelet op de beschikbare technologie) of de meerwaarde van het gebruik van nationale kopieën. Hij beveelt aan om te voorkomen dat de lidstaten nationale kopieën kunnen gebruiken, of om deze mogelijkheid op zijn minst sterk te beperken. Indien nationale kopieën worden ontwikkeld, dan moet het gebruik daarvan onderworpen worden aan een strikt beginsel van doelbeperking. Voorts mag de nationale kopie nooit op een andere manier worden aangezocht dan de centrale gegevensbank.

17. Wat de comitologie betreft: beslissingen die ingrijpende gevolgen hebben voor de gegevensbescherming, moeten in de vorm van een verordening of een besluit worden genomen, bij voorkeur in het kader van een medebeslissingsprocedure. Wanneer de comitologieprocedure wordt toegepast, moet de adviserende rol van de EDPS worden opgenomen in de artikelen 60 en 61 van het besluit en in artikel 35 van de verordening.

18. De invoering van interoperabiliteit tussen systemen mag niet inhouden dat het beginsel van de afbakening van het doel wordt geschonden, en elk voorstel op dit gebied moet aan de EDPS worden voorgelegd.

Gedaan te Brussel op 19 oktober 2005

Peter HUSTINX

Europees Toezichthouder voor gegevensbescherming