Permanente commissie
van deskundigen in
internationaal vreemdelingen-,
vluchtelingen- en strafrecht

Secretariaat
postbus 201, 3500 AE Utrecht/Nederland
telefoon 31 (30) 297 42 14/43 28
telefax 31 (30) 296 00 50
e-mail cie.meijers@forum.nl

[redacted] [redacted]

Aan De leden van Eerste en de Tweede Kamer der Staten-Generaal
Kenmerk CM03-13
Betreft Aanbieding van een notitie over de huidige voorstellen over het gebruik van Europese informatiesystemen (VIS, SIS II, biometrie) o.a. naar aanleiding van het punt 6 (Gemengd Comité) van de geannoteerde agenda voor de JBZ-Raad van 27 en 28 november 2003,

Datum 24 november 2003

Geachte leden,

Ten behoeve van uw overleg over aanstaande JBZ-Raad op 27 en 28 november 2003, biedt de Permanente Commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen- en strafrecht u, bijgevoegde notitie aan -met bijbehorende lijst met vragen- over de huidige voorstellen over het gebruik van Europese informatiesystemen (VIS, SIS II,biometrie).

Als punt 6 op de agenda van het Gemengd Comité staat het voorstel om een tweetal verordeningen aan te passen zodat reis- en verblijfsdocumenten voorzien mogen worden van biometrische kenmerken. Dit voorstel staat echter niet alleen. Een hele serie andere voorstellen bevinden zich eveneens in procedure, allen met het oogmerk om de kwaliteit, de gebruiksmogelijkheden en/of de kwantiteit van verzamelingen (digitale) persoonsgegevens te verhogen en om reden van het bestrijden van o.a. terrorisme en illegale immigratie. Bovendien heeft men bij de besluitvorming grote haast; voor het merendeel moet er vòòr het einde van 2003 overeenstemming bereikt te zijn over de voorstellen.

Door het hoge tempo waarmee deze gegevensverzamelingen worden ontwikkeld en de toenemende intensiteit van het uitwisselen van persoonsgegevens staan de normen die de bescherming van de persoonlijke levenssfeer regelen onder grote druk. Ook de beginselen van proportionaliteit en de aanwezigheid van een effectieve rechtsgang krijgen onvoldoende aandacht in de besluitvormingsprocedures binnen de EU. De grote druk om meer inlichtingenvergaring mogelijk te maken leidt er ook toe dat weinig aandacht is voor de vraag in hoeverre die grote nieuwe databestanden daadwerkelijk zullen bijdragen aan bescherming van de belangen die men beoogt te beschermen.

De Permamente Commissie hoopt met deze notitie de achtergrond en samenhang te kunnen schetsen van de talrijke (uitbereidings)voorstellen van gegevenssystemen. Daarnaast hoopt zij de principes en normen omtrent de bescherming van de persoonlijke levenssfeer weer de juiste plaats te geven in het besluitvormingsproces en het uiteindelijke resultaat daarvan.

De Permanente Commissie geeft u in overweging om de bij bijgaande notitie gevoegde lijst met vragen over de huidige voorstellen aan de Regering voor te leggen.

Namens de Permanente Commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen- en strafrecht,

hoogachtend,

Prof. mr. C.A. Groenendijk
voorzitter

Commentaar van de Permanente Commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen- en strafrecht inzake de huidige voorstellen inzake het gebruik van Europese informatiesystemen (VIS, SIS II, biometrie)

20 November 2003

1 Inleiding

In het najaar van 2003 onderhandelen de Europese regeringen over verschillende voorstellen om het gebruik en de opslag van persoonsgegevens uit te breiden. Deze voorstellen betreffen niet alleen de instelling van nieuwe verzamelingen van persoonsgegevens, maar ook het verbinden van deze systemen, de uitbreiding van gebruikers van de bestaande systemen en de opname van nieuwe categorieën gegevens daarin. De lidstaten willen niet alleen een biometrisch gegeven (in de vorm van vingerafdruk, gezichtsherkenning of irisscan) aan de Europese informatiebestanden toevoegen, maar deze ook opnemen in de verplichte reis- of identiteitsdocumenten. Hierdoor zal bij iedere grenspassage van een burger onmiddellijk gegevens over die persoon kunnen worden opgevraagd. Ten slotte staat er ook een Spaans voorstel op de Europese agenda voor een richtlijn inzake de verplichting van luchtvaartmaatschappijen om passagiersgegevens te verstrekken aan Europese grensautoriteiten. Zoals bekend, verplicht de Amerikaanse overheid nu al de Europese luchtvaartmaatschappijen om passagiersgegevens aan Amerikaanse grensautoriteiten te verstrekken.

Het is duidelijk dat deze ontwikkelingen met betrekking tot het gebruik en verwerking van persoonsgegevens gevolgen hebben voor de bescherming van individuele rechten. Personen, niet alleen derdelanders, maar ook EU onderdanen, zullen steeds vaker worden geconfronteerd met beslissingen waarop zij weinig tot geen controle kunnen uitoefenen. Beslissingen die zijn gebaseerd op het gebruik van informatiebronnen waarvan de betrouwbaarheid en objectiviteit zullen afnemen naarmate er meer staten, instanties of particuliere ondernemingen bij zijn betrokken.
De Europese regeringen hebben aangegeven dat zij eind 2003 politieke besluitvorming willen bereiken over onderwerpen als de tweede generatie van het Schengen Informatie Systeem (SIS II), het gemeenschappelijk Europees Visa Informatie Systeem VIS en de opname van biometrische gegevens. In dit commentaar formuleert de Permanente Commissie enkele belangrijke uitgangspunten die naar haar mening ten grondslag moeten liggen aan de komende besluitvorming. Omdat tot nu toe een duidelijk overzicht van de huidige ontwikkelingen ontbreekt, geeft zij eerst een korte samenvatting van de belangrijkste bestaande systemen en van de voorgestelde maatregelen.

2 Huidige ontwikkelingen en voorstellen

2.1 Operationele informatiesystemen in Europa

In het kader van de Europese grensoverschrijdende samenwerking worden op dit moment door middel van verschillende systemen persoonsgegevens opgeslagen en uitgewisseld. Het op dit moment grootste Europese informatiebestand is het Schengen Informatie Systeem (SIS). Deze databank bevat op dit moment meer dan 10 miljoen `signaleringen', waarvan bijna één miljoen signaleringen over personen. 90 % van die persoonssignaleringen betreffen derdelanders aan wie de toegang moet worden geweigerd. Naast personen die aan de grens moeten worden geweigerd en de op te sporen personen zoals getuigen en verdachten, bevat het SIS gegevens over voorwerpen (zoals vuurwapens en reisdocumenten).
Een andere grote database is het in 2003 operationeel geworden Eurodac. Dit bestand, dat vingerafdrukken bevat van asielzoekers, dient ter vaststelling van de voor de behandeling van een asielverzoek verantwoordelijke Europese staat, op basis van de zogenaamde Dublin II Verordening. In het kader van de strafrechtelijke en justitiële samenwerking zijn er voorts de analysebestanden van de Europese organisaties Europol en Eurojust.
Het recht op bescherming van persoonsgegevens is in verschillende Europese instrumenten neergelegd, welke instrumenten op de bovenbeschreven praktijk van toepassing zijn. In de eerste plaats is er het Verdrag van de Raad van Europa

inzake gegevensbescherming van 28 januari 1981.[1] (ook wel `Dataprotectieverdrag') Dit verdrag is van toepassing op zowel de gegevensverzameling van Europol en Eurojust en het SIS. Daarnaast is de Europese Richtlijn *inzake de bescherming van persoonsgegevens* van 24 oktober 1995[2] van toepassing op gegevensverwerking in communautair verband. Onder de reikwijdte van deze richtlijn valt bijvoorbeeld Eurodac. Belangrijk voor de erkenning van het recht op gegevensbescherming als een zelfstandig grondrecht is de recente opname van het recht op bescherming van persoonsgegevens in artikel 8 van het EU Grondrechten Handvest. Ten slotte biedt ook de jurisprudentie van het Europese Hof voor de Rechten van de Mens in het kader van artikel 8 EVRM, inzake het recht op privé leven, belangrijke aanknopingspunten voor de noodzakelijke waarborgen bij de omgang met persoonsgegevens door de overheid, zoals het beginsel van proportionaliteit en subsidiariteit, de vereiste aanwezigheid van een onafhankelijk toezichtmechanisme en het legaliteitsbeginsel.[3]

2.2 Uitbreiding van het huidige SIS

Met betrekking tot de uitbreiding van het huidige SIS liggen in 2003 enkele concrete voorstellen voor akkoord bij de Raad. Deze voorstellen beogen slechts aanpassingen van het huidige systeem. In de eerste plaats is daar het Spaanse voorstel voor een verordening en een besluit voor de uitbreiding van de functionaliteiten van het SIS ten behoeve van terrorismebestrijding.[4] Dit voorstel voorziet in de (beperkte) toegang tot het SIS voor Europol en Eurojust; de regeling van een juridische basis van Sirene (de organisatie die additionele informatie aan de nationale autoriteiten verstrekt bij de bovengenoemde SIS signaleringen), en de regeling van de bewaartermijnen van de Sirene gegevens. Ten slotte bevat dit voorstel ook enkele aanvullend op te nemen persoonsgegevens (bijvoorbeeld of iemand ontsnapt of gewapend is). Ten tweede heeft de Commissie in augustus 2003 een voorstel ingediend voor een verordening op grond waarvan nationale organisaties belast met de afgifte van kentekenbewijzen toegang kunnen krijgen tot bepaalde categorieën gegevens (gestolen voertuigen en documenten) in het SIS.[5]

2.3 SIS II

Algemene en meer ingrijpende veranderingen vinden echter plaats onder de noemer van het ‘SIS II’. De besluitvorming rond het SIS II is oorspronkelijk bedoeld om het SIS technisch gebruiksklaar te maken voor een groter aantal landen. Deze wijziging is nodig met het oog op de toetreding van nieuwe EU landen in 2004. De praktische reden om het SIS te wijzigen is echter aangegrepen om ook te onderhandelen over nieuwe doeleinden van het SIS; over nieuwe categorieën op te nemen gegevens en over nieuwe gebruikers van het SIS.[6] De lidstaten willen het SIS II eind 2006 gereed hebben voor gebruik voor alle EU lidstaten. Om deze datum te halen, zouden eind 2003 de besluiten moeten worden genomen over de voorgestelde functionele wijzigingen van het SIS.

De belangrijkste voorstellen die op dit moment in de onderhandelingen over het SIS II spelen zijn:

- het verlaten van het huidige zogenaamde *‘hit - no hit’* systeem. Op dit moment wordt bij het aantreffen van een bepaald object of persoon in het SIS, een welomschreven actie van een bepaalde autoriteit gevraagd. De huidige voorstellen lijken van het SIS een meer proactief informatiesysteem te maken. In plaats van alleen een meldingssysteem, zal het SIS een meldings- èn onderzoekssysteem worden.[7] Zo wordt voorgesteld om niet alleen gegevens op te nemen over personen die voor concrete doeleinden of acties

[1] ETS, nr. 108.
[2] 95/46/EC, *OJ* L 281/31.
[3] Zie o.a. het Leander arrest, EHRM, 26 maart 1987, Series A, no.116; Amann vs. Switzerland, 16 February 2000, Report of Judgements and Decisions 2000-II; ECtHR, 7 July 1989, Series A , no. 160; en Rotaru vs. Romania, 4 May 2000 ECtHR 2000-V.
[4] *OJ* 2002, C 160.
[5] COM (2003) 510.
[6] Zie ondermeer de mededeling over SIS II van de Commissie, COM (2001) 720.
[7] Zie de Commissie, die reeds in 2001 ervoor waarschuwde dat de opzet van het SIS fundamenteel zou wijzigen. COM (2001) 720, p. 8.

worden gezocht, maar ook informatie over personen die mogelijk strafbare feiten zullen plegen, of mogelijk een gevaar voor de openbare orde of nationale veiligheid inhouden.
- de wijziging van de huidige architectuur: het huidige systeem bestaat uit een centraal systeem (CSIS), met in alle landen exacte kopieën van dat centrale systeem in de vorm van NSIS. Deze nationale SIS bestanden zijn gebonden aan de algemene Schengen regels inzake gegevensbescherming die zijn neergelegd in de Schengen Uitvoeringsovereenkomst. Het huidige recht verbiedt Schengen staten om de SIS gegevens die door andere staten zijn ingebracht te kopiëren naar overige nationale bestanden. De Commissie stelt nu voor om één centrale database in te richten, waartoe nationale gebruikers via zogenaamde *'interfaces'* direct toegang krijgen.[8] Het opslaan van de SIS gegevens in nationale bestanden zou dan, volgens de Commissie, onder de eigen verantwoordelijkheid van die staten vallen.
- koppeling van verschillende gegevensverzamelingen: hierboven zagen we reeds dat de autoriteiten van de Europese organisaties Europol en Eurojust binnenkort rechtstreeks toegang krijgen tot bepaalde categorieën SIS gegevens. In het kader van het SIS II wordt echter ook de mogelijkheid besproken om SIS direct met andere Europese systemen te verbinden, zoals met de Sirene-gegevensverzameling, met Eurodac of met het toekomstige VIS. In sommige Europese stukken wordt zelfs gesproken van de mogelijkheid om de verschillende systemen te integreren in één Europees Informatie Systeem.[9]
- voorstel om zogenaamde "*interlinking van alerts*" mogelijk te maken: nu hebben van te voren vastgestelde autoriteiten slechts toegang tot bepaalde categorie gegevens. Interlinking zou het mogelijk maken dat een gebruiker die slechts toegang heeft tot een bepaalde categorie gegevens in verband met zijn functie, ook toegang krijgt tot andere aanwezige alerts over de gezochte persoon in het SIS, ook al heeft de gebruiker in verband met zijn functie primair geen toegang tot deze gegevens.
- landen als de Verenigde Staten, maar ook buurlanden van nieuwe EU staten hebben al hun belangstelling voor de door de Europese staten opgeslagen persoonsgegevens getoond. Ook over de toegang van deze derde staten zal een besluit moeten worden genomen.
- toegang van het Verenigd Koninkrijk en Ierland: ook al participeren deze landen op dit moment niet in de EU samenwerking op het gebied van asiel en migratie, op grond van het Raadsbesluit 2000/365/EG zullen deze landen wel toegang tot het SIS krijgen voor wat betreft de justitiële en politiële gegevens. Onderhandelingen vinden echter ook plaats over de toegang van deze landen tot gegevens over visa en te weigeren vreemdelingen.[10]
- beheer en plaats van het SIS: op dit moment is het centrale SIS (CSIS) gesitueerd in Straatsburg en valt het onder beheer van Raad. Het Europees Parlement en de Commissie stellen voor om het SIS door een zelfstandig agentschap te laten beheren.

2.2 Visum Informatie Systeem (VIS)

Het VIS betreft het voorstel voor een centrale Europese database waarmee informatie over visa die door de EU staten zijn verstrekt of geweigerd kan worden uitgewisseld. Dit systeem zou niet alleen de gegevens moeten gaan bevatten over de afgegeven visa, maar ook over iedere visumaanvraag èn visumweigering. In juni 2002 hebben de ministers van Justitie en Binnenlandse Zaken reeds richtsnoeren aangenomen voor de instelling van een gemeenschappelijk systeem voor de uitwisseling van informatie over visa.[11] Uit de in deze richtsnoeren genoemde doeleinden kan men afleiden dat het toekomstige VIS een multifunctioneel systeem moet worden.[12]

---

[8] Zie de Commission Staff Working Paper inzake de ontwikkeling van SIS II van 18 februari 2003, SEC (2003) 206, opgenomen in het Raadsdocument 6615/03.
[9] In een nota van het EU voorzitterschap inzake derde pijler informatiesystemen wordt als een mogelijke optie voor de lange termijn genoemd 'het samen brengen van alle bestaande systemen in één "Unie Informatie Systeem" zodat aan alle toekomstige behoeftes in alle relevante gebieden voldaan kan worden', doc. 8857/03 van 6 mei 2003. Ook het EP rapport inzake de tweede generatie Schengen Informatie Systeem van de rapporteur Carlos Coelho, noemt de mogelijkheid van één geïntegreerd systeem, A5-0398/2003, 7 november 2003.
[10] Zie de nota van het Verenigd Koninkrijk van 25 maart 2003, Raadsdocument 7786/03.
[11] Zie Raadsdoc. 9615/02 van 5 juni 2002.
[12] Zie ook de mededeling van de Commissie over een gemeenschappelijk beleid

Zo worden als doeleinden van het VIS genoemd:

- de vergemakkelijking van fraudebestrijding door middel van betere uitwisseling van informatie inzake visumaanvragen tussen de lidstaten (overigens is niet aangegeven welke fraude is bedoeld);
- betere consulaire samenwerking op lokaal niveau en uitwisseling van gegevens tussen centrale autoriteiten die bevoegd zijn voor consulaire samenwerking;
- de verbetering van de methode om vast te stellen of de bezitter van een visum en de wettige houder ervan één en dezelfde persoon zijn;
- de bestrijding van het zogenaamde 'visumshopping'(wanneer een aanvrager, na weigering door één consulaat, bij een consulaat van een andere lidstaat een visumverzoek indient);
- het vereenvoudigen van identificatie in het kader van de Dublin II Verordening en terugkeerprocedures;
- een beter beheer van een gemeenschappelijk visumbeleid en;
- het leveren van een bijdrage aan de interne veiligheid en bestrijding van terrorisme.

De Raad wil in december 2003 een politiek akkoord bereiken over de basiselementen van VIS, zoals:

- de architectuur: een systeem vergelijkbaar met het huidige SIS (dus een centrale opzet met nationale kopieën in iedere lidstaat), of een systeem dat is geïntegreerd met het SIS, of een geheel nieuwe structuur;
- de vaststelling van de definitieve doeleinden;
- een regeling van gebruikers;
- de toegang voor derde staten en;
- de opname (en de keuze) van biometrische gegevens.

2.3 Opname biometrische gegevens

In september 2003 heeft de Commissie voorstellen ingediend die het mogelijk maken om biometrische gegevens op te nemen in zowel de visa, als de verblijfsdocumenten van derdelanders.[13] In deze voorstellen geeft de Commissie de voorkeur aan de opname van (twee) vingerafdrukken en een digitale fotoafdruk. Daarnaast bereiden Europese lidstaten op nationaal niveau reeds wetgeving voor ter opname van biometrische gegevens in alle identiteitsdocumenten, dus ook van EU onderdanen. Deze wetgeving vloeit voort uit een maatregel die de Amerikaanse overheid heeft ingevoerd na de gebeurtenissen van 11 september 2001. Op basis van deze maatregel dienen alle landen waarvan de onderdanen van een visum zijn vrijgesteld, de reisdocumenten van hun onderdanen van biometrische gegevens te voorzien. Gebeurt dit niet dan vervalt voor dat land de visumvrijstelling op basis van het zogenaamde Amerikaanse Visa Waiver Program. De Europese Commissie heeft inmiddels aangekondigd dat zij voorstellen zal indienen voor de opname van veiligheidskenmerken, waaronder biometrische gegevens, in de EU paspoorten.[14] Daarnaast onderhandelen de lidstaten, zoals we hierboven al zagen, over de opname van biometrische gegevens in zowel het SIS II als het VIS.[15] Bij deze discussie lijkt het echter niet zozeer te gaan over de vraag òf deze gegevens wel in een centrale informatiebestand mogen worden opgenomen, maar meer over de vraag wèlke categorie van biometrische gegevens zal worden opgenomen.

3 Algemene kritiekpunten

3.1 Gebrek aan democratische en inhoudelijke legitimatie

Een goede besluitvorming vereist een openbare afweging van nut en effectiviteit van voorgestelde systemen enerzijds, tegenover de financiële kosten en de bescherming van individuele rechten anderzijds. De Europese bewindslieden geven aan dat de politieke besluitvorming over de bovenbeschreven onderwerpen eind 2003 moet zijn afgerond. De EU lidstaten lijken echter al over de principiële

---

inzake illegale immigratie, mensen handel en mensensmokkel, COM (2003) 323, juni 2003.
[13] Voorstel van 25 september 2003, COM (2003) 558.
[14] COM (2003) 323, 3 juni 2003, p. 6.
[15] Zie bijvoorbeeld Raadsdocument 10857/03.

punten, zoals de invoering van het VIS, de uitbreiding van de taken van het huidige SIS en het gebruik van biometrie hun besluiten te hebben genomen, zonder dat hier enig parlementair debat aan vooraf is gegaan. Een structureel en publiek debat over concrete voorstellen ontbreekt: mondjesmaat worden door hetzij de Commissie, hetzij de verschillende lidstaten, voorstellen gedaan over mogelijk doelen, categorieën op te nemen gegevens of gebruikers van de toekomstige systemen. De haalbaarheidstudie inzake het VIS die de Commissie in mei 2003 aan de Raad heeft gestuurd, is tot nu toe niet publiek gemaakt. Hierdoor blijft het onhelder of, en zo ja welke afweging er is gemaakt tussen enerzijds de verwachte voordelen van het VIS, en anderzijds de betrokken rechten en belangen van individuen. Er dreigt een legitimatie achteraf plaats te vinden van een materie die niet alleen zeer ingewikkeld is, maar ook ingrijpende gevolgen kan hebben voor de rechten en vrijheden van Europese burgers en derdelanders.
De besluitvorming over het opzetten van nieuwe informatiesystemen of het uitbreiden van de huidige systemen vereist een voorafgaande evaluatie van de bestaande instrumenten. Lidstaten zullen moeten aangeven wat het effect van de bestaande instrumenten is, en waar deze instrumenten met het oog op de gestelde doelen falen. Pas na zo een evaluatie kan, in een democratisch kader en in nauw overleg met de nationale en internationale toezichtorganen inzake de gegevensbescherming, een afgewogen besluit worden genomen over nieuwe maatregelen. Wat betreft het gebruik van het huidige SIS, wordt meermalen verwezen naar het nut van dit systeem, ondermeer gezien het groot aantal hits (dat wil zeggen, dat een gebruiker een bepaalde persoon aantreft in het systeem). Openbare cijfers over de bijdrage die deze hits daadwerkelijk leveren aan de bestrijding van criminaliteit of aan andere met het SIS gestelde doeleinden, zijn er niet. Een belangrijk probleem ten aanzien van het huidige SIS is het ontbreken van openbare rapporten over het functioneren van dit systeem. De jaarverslagen van het bij het SIS ingestelde toezichtorgaan, de Gemeenschappelijke Controle Autoriteit (GCA), geven wel enig inzicht in het gebruik van het SIS, maar bestrijken slechts een deelaspect van het gebruik van het SIS, namelijk de gegevensbescherming.
Ook wat betreft de voorgestelde opname van biometrische gegevens is onvoldoende onderbouwd wat het precieze doel en meerwaarde is van deze opname. De lidstaten geven niet aan wat de gevolgen van het gebruik van biometrie zijn, noch in hoeverre de betrouwbaarheid van deze gegevens kan worden gegarandeerd. In dit kader zijn de recente kanttekeningen van belang, die de Groep Gegevensbescherming Artikel 29, een Europees adviesorgaan op het gebied van gegevensbescherming, bij het opslaan van biometrische gegevens heeft geplaatst.[16] In een advies van augustus 2003 geeft de werkgroep expliciet aan dat ieder besluit over gebruik van biometrie aan het proportionaliteitsvereiste moet voldoen. Ook adviseert de werkgroep om biometrische gegevens niet in een centrale databestand op te nemen. Bovendien verwijst dit advies naar verschillende kritische besluiten inzake het gebruik van biometrie van nationale gegevensbeschermingsautoriteiten.

3.2 Gebrek aan transparantie van huidige regelgeving inzake gegevensbescherming

De EG Richtlijn 95/46 inzake gegevensbescherming is niet van toepassing op het SIS omdat de rechtsgrondslag van het SIS berust op de huidige derde pijler van het EU Verdrag en de genoemde richtlijn alleen van toepassing is op communautaire gegevensverwerking. De Commissie geeft aan dat met het oog op de opheffing van het verschil tussen de drie pijlers in het kader van het ontwerp Constitutioneel Verdrag, SIS II in de toekomst één rechtsbasis, met ook één regeling voor de gegevensbescherming dient te krijgen. Zolang echter de besluitvorming rond het Constitutioneel Verdrag niet is afgerond, zal de Commissie de wetgevingsvoorstellen inzake het SIS II nog op twee rechtsgrondslagen baseren.
Zoals we hierboven zagen is de EG Richtlijn wel van toepassing op Eurodac. Gezien de toekomstige functie van het VIS, zal deze ook onder de reikwijdte van de EG Richtlijn vallen. Hierdoor ontstaat een vreemde tweedeling tussen de normen van het Dataprotectieverdrag van de Raad van Europa en de daarop gebaseerde aanbevelingen enerzijds en de communautaire regels inzake gegevensbescherming anderzijds. Bovendien hebben systemen als het SIS, Europol

[16] Werkdocument over biometrie, aangenomen op 1 augustus 2003, 12168/02/NL WP 80. De Groep Gegevensbescherming Artikel 29 is op basis van artikel 29 van de EG Richtlijn 95/46 ingesteld.

en Eurodac ook nog eens hun eigen regelingen inzake gegevensbescherming met een afzonderlijk toezichtmechanisme. Dit naast elkaar bestaan van verschillende dataprotectie regimes komt de transparantie van het toepasselijke recht niet ten goede. De opname van het recht op bescherming van persoonsgegevens in artikel 8 van het EU Handvest is een belangrijke stap naar de erkenning van een pijleroverschrijdend individueel grondrecht op een adequate gegevensbescherming. Artikel 50 van het ontwerp Constitutioneel Verdrag bevat bovendien de opdracht aan de EU wetgever om één EU regeling inzake gegevensbescherming op te stellen en één autoriteit te belasten met de gegevensbescherming. Tijdens de Raad van juni 2003 is er al een Grieks voorstel aan de Raad voorgelegd om eenvormige regels voor de derde pijler te ontwikkelen. Tot nu toe lijkt de Raad echter weinig gevolg aan dit voorstel te geven. Ten behoeve van de transparantie voor de burgers zou het de aanbeveling verdienen wanneer gegevensverwerking en informatiesystemen onder één gemeenschappelijke kader van gegevensbescherming komen. Deze algemene regels zouden dan per sector of onderwerp kunnen worden uitgewerkt in meer specifieke regels.

4 Concrete aanbevelingen

4.1 Doelbindingsbeginsel

Eén van de belangrijkste uitgangspunten van gegevensbescherming is het doelbindingsbeginsel. Dit houdt in de eerste plaats in dat de EU lidstaten alleen gegevens mogen verwerken (verzamelen, gebruiken en opslaan) voor een specifiek, expliciet en legitiem doel. De lidstaten moeten bij ieder besluit op het gebied van de verwerking van persoonsgegevens expliciet aangeven, niet alleen wat het doel van deze gegevensverwerking is, maar ook waarom het gekozen instrument tot het beoogde doel bijdraagt. Deze motiveringsplicht vloeit ook voort uit de beginselen van noodzakelijkheid en proportionaliteit, zoals die zijn geformuleerd door het Europese Hof voor de Rechten van de Mens in jurisprudentie rond artikel 8 EVRM.[17]
Daarnaast betekent het doelbindingsbeginsel dat opgeslagen of verzamelde persoonsgegevens niet voor andere doeleinden mogen worden gebruikt. Naleving van dit beginsel zal moeilijker te garanderen zijn, naarmate het informatiesyteem grootschaliger is en naarmate er meer staten en autoriteiten van gebruik maken. Bij de besluitvorming over toekomstige systemen moeten de lidstaten dit aspect expliciet meewegen.

4.2 Op te nemen gegevens

Op grond van het genoemde doelbindingsbeginsel dienen de te verwerken gegevens adequaat, relevant en niet excessief te zijn in het licht van het beoogde doel.[18] Dit betekent dat de lidstaten voor iedere categorie gegevens die zij in Europese databanken willen opnemen, de relevantie en proportionaliteit moeten vaststellen, in het licht van het doel waarvoor deze gegevens zullen worden gebruikt. Daarbij is het soort gegevens dat mag worden opgenomen, afhankelijk van de aard en reikwijdte van het beoogde gebruik van deze gegevens. Hoe ruimer het gebruik en hoe meer autoriteiten toegang hebben tot het systeem, des te strenger de eisen met betrekking tot de adequaatheid en juistheid van de gegevens zullen moeten zijn.

In het kader van het SIS II, maar eventueel ook van het VIS, moet een principiële keuze worden gemaakt tussen een systeem van wederzijdse erkenning van nationale beslissingen om iemand in een systeem op te nemen, of een systeem waarbij de criteria voor de opname van een persoon (of object) in een systeem volledig zijn geharmoniseerd. Op dit moment kent het SIS een gemengd systeem. De regeling van het SIS, de Schengen Uitvoeringsovereenkomst, beschrijft de basiscriteria waaraan personen (of objecten) moeten voldoen en voor welke doeleinden ze in het SIS mogen worden opgenomen. Deze criteria zijn echter vaag en laten ruimte voor verschillen in invulling door de Schengenstaten. Daarnaast is de regeling van het SIS gebaseerd op het beginsel van wederzijdse erkenning. Bijvoorbeeld wanneer één staat een vreemdeling op nationale gronden toegang tot het grondgebied wil weigeren en deze persoon daartoe in het SIS opneemt, dan zal deze persoon ook de toegang tot alle andere Schengenstaten moeten worden geweigerd.

---

[17] Zie noot 3
[18] Zie bijvoorbeeld artikel 6 (c) EG Richtlijn 95/46.

De nationale verschillen in de uitvoering en het gebruik van het SIS bemoeilijken de controle door toezichtorganen of rechtspraak. Daarnaast kleeft aan het systeem van wederzijdse erkenning het nadeel van ondoorzichtigheid en een mate van willekeur tegenover de persoon die in het systeem wordt opgenomen. Duidelijke, nauwkeurig omschreven criteria voor opname van gegevens in een Europees informatiesysteem verdienen daarom de voorkeur boven een systeem van wederzijdse erkenning van nationale besluiten.
Met name in de nasleep van de gebeurtenissen van 11 september 2001, zijn in het kader van de discussie rond SIS II door de afzonderlijke lidstaten verschillende voorstellen gedaan ter opname van nieuwe categorieën gegevens. De voorgestelde categorieën variëren van *'gewelddadige ordeverstoorders'*, *'potentieel gevaarlijke personen die van bepaalde evenementen moeten worden uitgesloten'*, en *'personen ten aanzien van wie moet worden voorkomen dat ze het Schengen gebied verlaten'.*[19] Maar ook het huidige criterium in artikel 96 Schengen Uitvoeringsovereenkomst*, 'vreemdelingen die een gevaar voor de openbare orde en veiligheid of de nationale veiligheid kunnen opleveren'* is vaag. Het laat toe dat personen in het SIS worden opgenomen, louter en alleen op basis van een vermoeden, zonder dat hiervoor aan nadere criteria moet zijn voldaan. Het is belangrijk dat grootschalige, multifunctionele informatiesystemen enkel zogenaamde *'harde gegevens'* bevatten, dat wil zeggen informatie waarvan vooraf is getoetst dat die een werkelijke situatie of eigenschap weergeeft en die niet is gebaseerd op vermoedens of op het gebruik van zogenaamde profielen. Zogenaamde *'zachte'* informatie, die opsporings- of veiligheidsdiensten nodig hebben bij hun taken, horen thuis in aparte (analyse-) bestanden, waarvan de gebruiker van te voren weet dat deze informatie nader moet worden getoetst. Deze informatie mag alleen worden gebruikt voor verder onderzoek en niet voor vervolging of weigering aan de grens.

4.3 Gebruikers – toegang aan derden

In de huidige onderhandelingen over SIS II worden voorstellen gedaan ter uitbreiding van gebruikers van het SIS: zowel met nationale autoriteiten als met derde staten. Het huidige SIS is gebaseerd op het principe dat een van tevoren vastgestelde groep gebruikers slechts toegang heeft tot bepaalde categorieën van gegevens, waarvan van tevoren is vastgesteld dat zij die voor de uitvoering van hun taak nodig hebben. Dit beginsel dient ook het uitgangspunt te blijven bij het toekomstige SIS, maar ook bij andere toekomstige informatiesystemen. Voor de transparantie naar de burger is het bovendien noodzakelijk dat wanneer besluiten zijn genomen over de gebruikers, de lidstaten de lijsten met deze gebruikers aan hun nationale en het Europees parlement overleggen of anderszins openbaar maken.

Wanneer SIS II, en eventueel VIS, onder een zelfstandig agentschap wordt gebracht, zoals is voorgesteld door het Europese Parlement en de Commissie, is het van belang dat een dergelijk agentschap niet de bevoegdheid krijgt om zelfstandig toestemming te verlenen voor doorgifte van de SIS gegevens aan derde staten of instanties. Gegevensverstrekking aan derden mag uitsluitend geschieden op basis van duidelijke criteria aan bepaalde vooraf vastgestelde instanties, neergelegd in een Verdrag of ander adequaat rechtsinstrument. De besluitvorming hierover moet in een democratisch kader en in overleg met toezichtorganen voor de gegevensbescherming plaatsvinden. Dit voorkomt dat het gebruik van het SIS of het VIS volkomen ondoorzichtig wordt voor democratische controle door discretionaire bevoegdheden te verlenen aan hetzij een agentschap, hetzij de nationale overheden.
Het uitgangspunt van Europese samenwerking op het gebied van gegevensuitwisseling is steeds geweest dat de andere Europese staten waaraan de gegevens worden uitgewisseld, een gelijk niveau van gegevenbescherming bieden. Met betrekking tot de gegevensverstrekking aan derde, niet Europese staten, vereist de Europese richtlijn dat deze staten over een adequaat gegevensbeschermingsniveau beschikken. Dit betekent dat ook aan toekomstige gegevensverstrekking aan derde staten strenge eisen moeten worden gesteld, zoals: de eis dat gegevensuitwisseling enkel mag plaatsvinden op basis van een concreet verzoek met toetsing door een toezichthoudend orgaan; dat de ontvangende staat de garantie moet bieden dat de gegevens voor een beperkt en concreet doel worden gebruikt; en dat het individu dient te worden geïnformeerd over de gegevensverstrekking aan derde staten of instanties. Tot slot zou het

[19] Zie ondermeer de volgende Raadsdocumenten: 6164/1/01, 14790/01 en 5968/02. Zie ook de conclusies in doc. 9808/03 die tijdens de Raad van Ministers van Justitie en Binnenlandse Zaken van 5-6 juni 2003 zijn goedgekeurd.

aanbeveling verdienen wanneer dergelijke afspraken over gegevensverstrekking aan derde staten op basis van wederkerigheid geschieden.

4.4 Bewaartermijnen

Voor het huidige SIS geldt dat gegevens over personen drie jaar mogen worden bewaard, met uitzondering van personen die voor onopvallende of gerichte controle zijn opgenomen: daarvoor geldt een termijn van één jaar. Echter wanneer de nationale overheid langere bewaring noodzakelijk acht, kan zij de termijn steeds verlengen. In een bijeenkomst van 20 juni 2002 oordeelde de Raad nog dat verlenging van bewaartermijnen niet nodig is omdat de huidige SIS regeling aan de bestaande behoeften voldoet.[20] Een jaar later echter besluit de Raad, in een andere samenstelling, dat bij de beslissingen over nieuwe functies van het SIS, óók een besluit moet worden genomen over wijziging van de bewaartermijnen.[21] Concrete voorstellen zijn, voor zover bekend, nog niet gepubliceerd. Ten aanzien van het VIS is in 2002 een bewaartermijn van vijf jaar voorgesteld, met de mogelijkheid van verlenging.[22]
Om het gebruik van verouderde, onbruikbare gegevens te voorkomen, zal per categorie gegevens en per doel waarvoor die gegevens worden opgeslagen, een passende bewaringstermijn moeten worden vastgesteld. De vaststelling van deze bewaartermijnen moet in overleg met de onafhankelijk toezichtorganen geschieden. Verlenging van deze termijn mag niet automatisch gebeuren, maar dient per concreet geval te worden gemotiveerd. Naleving van de bewaartermijnen dient periodiek getoetst te worden door het onafhankelijk toezichtorgaan, op Europees of op nationaal niveau.

4.5 Individuele rechten

De burger heeft het recht op informatie over het gebruik van zijn of haar persoonlijke gegevens. Dit vergroot niet alleen het draagvlak voor de voorgestelde systemen bij de burgers, maar ook de efficiency en juistheid van de gebruikte systemen. Door de uitoefening van dit recht kunnen immers ook foute en onterecht opgenomen gegevens worden opgespoord en gecorrigeerd. De autoriteiten moeten de burger zoveel mogelijk vooraf informeren over het gebruik van zijn of haar persoonsgegevens. De verstrekte informatie moet zowel duidelijkheid bieden over het voorgenomen doel van de gegevensopslag, wie de gebruikers zijn van die informatie, wat de bewaartermijnen zijn en ten slotte welke rechten en rechtsmiddelen de betreffende persoon heeft. Deze informatie moet bij voorkeur worden verstrekt op het moment van afname van de betreffende gegevens of op het moment wanneer deze gegevens in een informatiesysteem worden opgenomen. Bij de afname van biometrische gegevens zal de betreffende persoon in ieder geval op het moment van afname over het doel en het gebruik moeten worden geïnformeerd. Wanneer bij een grensovergang of anderszins, gezichts- of irisherkenning wordt gebruikt als biometrisch identificatiemiddel, dan moeten de autoriteiten de aldus gecontroleerde personen steeds inlichten over het moment en de wijze waarop zij worden gecontroleerd.

4.6 Effectieve rechtsmiddelen

Aan de in de Europese informatie systemen opgenomen persoon moeten effectieve rechtsmiddelen open staan. Dit kan hetzij door eenvoudige toegang te bieden tot een nationaal of Europees toezichtorgaan, onder voorwaarde dat dit orgaan over bindende bevoegdheden beschikt, hetzij door toegang te bieden tot een nationale rechter. Bij toegang tot een nationale rechter verdient het de voorkeur om het systeem van het huidige SIS te kiezen, waarbij een individu zelf kan kiezen op welk grondgebied het een procedure wil starten. Het rechtsmiddel moet openstaan ten aanzien van zowel het besluit om iemand in een informatiesysteem op te nemen, als ten aanzien van het besluit dat op basis van een in een systeem opgenomen informatie is genomen. Een besluit met rechtsgevolgen voor de geregistreerde moet dus mede op de juistheid van die gegevens kunnen worden getoetst.

---

[20] Zie de notulen van de Ecofin Raad, Raadsdocument 10089/02 (Press 181) en ook een eerdere nota van het EU voorzitterschap, doc. 13269/01, 31 oktober 2001.
[21] Zie eerdergenoemd doc. 9808/03.
[22] Zie doc. 9615/02 van 5 juni 2002.

De huidige regeling in de Schengen Uitvoeringsovereenkomst bepaalt dat iedere uitspraak van een nationale rechter of toezichtinstantie in verband met de rechtmatigheid van gegevensverwerking, moet worden nageleefd door de nationale autoriteiten van iedere andere lidstaat. Het verdient aanbeveling om voor een vergelijkbare regeling te kiezen bij SIS II en het VIS.

4.7 Internationaal toezichtorgaan

Op dit moment bestaan er op Europees niveau verschillende toezichtmechanismen. In de eerste plaats wordt toezicht op nationaal niveau uitgevoerd: bijvoorbeeld bij het SIS houden nationale dataprotectie autoriteiten toezicht op gebruik van de nationale SIS systemen. De wijze waarop dit toezicht wordt uitgeoefend kan verschillen, omdat dit nationaal verschillend is geregeld. Daarnaast hebben het SIS, Europol en Eurodac ieder hun eigen gemeenschappelijke toezichthoudende autoriteit. Wel is voor deze autoriteiten met een besluit van oktober 2000 een gemeenschappelijke secretariaat gecreëerd.[23] Op korte termijn zal een Europees toezichthoudend orgaan worden aangesteld. Dit orgaan is echter alleen belast met het toezicht op de uitvoering van het Europese gegevensbeschermingsrecht door de Europese instanties en lichamen zelf. Hoewel het bestaan van deze Europese autoriteiten is toe te juichen, biedt het geheel van deze verschillende toezichtmechanismen, een versnipperd en ondoorzichtig beeld.
Er dient op Europees niveau één orgaan te worden ingesteld dat toezicht houdt op de persoonsinformatiesystemen die op basis van Europees recht zijn ingesteld en die door de nationale autoriteiten van de EU lidstaten worden gebruikt. Dit Europees toezichtorgaan kan eventueel worden toegerust met gespecialiseerde kamers voor de afzonderlijke Europese informatiesystemen. Het toezichtorgaan dient in ieder geval voldoende financiële middelen te krijgen om haar taken naar behoren uit te voeren. Ook moet ze worden toegerust met bindende instrumenten, zoals bijvoorbeeld de mogelijkheid een instantie te verplichten tot verwijdering of correctie van gegevens; de bevoegdheid boetes op te leggen; en te bevelen dat gegevensverwerking bij ernstige schending van de regelgeving wordt stopgezet.

4.8 Opname evaluatieplicht

Het noodzakelijk om in de wettelijke regeling van ieder toekomstig informatiesysteem een evaluatieplicht op te nemen. Deze evaluatie moet de effecten wat betreft gebruik, behaalde doelen, rechtsbescherming en kosten bestrijken. De evaluatie dient te worden uitgevoerd binnen een bepaalde termijn (bijvoorbeeld twee jaar) na het operationeel worden van het informatiesysteem.

5 Conclusie

De noodzaak van de opheffing van de interne grenscontroles werd in 1985 door de Europese Commissie in haar Witboek over de interne markt nog gemotiveerd met de overweging: ‘Grenscontrole komt op de burger over als de veruitwendiging (sic) van een willekeurige administratieve macht die boven de individuen staat’.[24]
Inmiddels, anno 2003, is de vraag gerechtvaardigd of de maatregelen die op het gebied van het gebruik van persoonsinformatie ten behoeve van de grenscontrole worden voorgesteld, niet veel meer als een willekeurige administratieve macht zullen worden ervaren.
Bij de komende besluitvorming zullen de lidstaten met name de beginselen van proportionaliteit en subsidiariteit in het oog moeten houden. Inachtneming van de hier boven genoemde minimumvoorwaarden draagt niet alleen bij aan het vertrouwen van de burger in de (Europese) overheid, maar ook aan een effectieve en transparante uitvoering van de door die overheid gestelde taken.

[23] Raadsbesluit van 17 oktober 2000, *OJ* L271, 24.10.2000.
[24] COM 1985 (310), juni 1985, overweging nr. 48, p. 14.

Vragen behorende bij het Commentaar van de Permanente Commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen- en strafrecht inzake de huidige voorstellen inzake het gebruik van Europese informatiesystemen (VIS, SIS II, biometrie)

1. Inhoudelijke en democratische legitimatie

- Is de regering het met de Permanente Commissie eens dat de besluitvorming over het opzetten van nieuwe informatiesystemen of het uitbreiden van de huidige systemen een voorafgaande evaluatie van de bestaande instrumenten vereist?
- Kan de regering het parlement een overzicht geven over wat het effect van huidige systemen als het SIS en Eurodac is, en waar deze instrumenten met het oog op de gestelde doelen falen? Kan de regering aangeven welke bijdrage het huidige SIS bijvoorbeeld levert aan de bestrijding van criminaliteit of van illegale immigratie?
- Op grond van welke afwegingen willen de EU lidstaten het gebruik van het huidige SIS uitbreiden?
- Kan de regering aangeven hoeveel gegevens op dit moment in Eurodac zijn opgeslagen, en hoeveel gegevens er dagelijks in worden opgenomen? Kan de regering al aangeven in hoeverre dit systeem bijdraagt aan de uitvoering van de Verordening inzake de vaststelling van een voor een asielverzoek verantwoordelijke staat?
- Kan de regering aangeven welke afweging er is gemaakt tussen enerzijds de verwachte bijdragen van een toekomstig VIS aan de gestelde doelen, en anderzijds de nadelen van een dergelijk grootschalig systeem: zoals hoge kosten, gevolgen voor de rechten en vrijheden van het individu, misbruikgevoeligheid?
- Kan de regering de haalbaarheidstudie inzake het VIS, zoals deze in het voorjaar 2003 door de Commissie aan de Raad is gepresenteerd, alsnog voor het parlement toegankelijk maken? Deelt de regering de mening dat openbaarheid van dit rapport een bijdrage levert aan de democratische besluitvorming?
- Wordt ieder nieuw voorstel inzake de opslag en het gebruik van persoonsgegevens getoetst aan het subsidiariteitsvereiste?
- In een brief aan de Tweede Kamer, eerder dit jaar (Vergaderjaar 2002-2003, 22 112, nr. 277) gaf de regering aan dat zij het Spaanse voorstel inzake de verplichting voor luchtvaartmaatschappijen om gegevens aan grensautoriteiten te verstrekken niet steunt, ondermeer omdat dit voorstel niet aan de eis van subsidiariteit voldoet. Staat de regering nog steeds afwijzend tegenover dit voorstel? Kan de regering aangeven wat het standpunt van de andere EU landen is over dit voorstel?
- Wil de regering er zorg voor dragen dat de besluitvorming over het opzetten van nieuwe informatiesystemen en het gebruik van biometrie, steeds in een democratisch kader en in nauw overleg met de nationale en internationale toezichtorganen inzake de gegevensbescherming plaatsvindt?

2. Transparantie

- Deelt de regering de mening van de Permanente Commissie dat de huidige regeling van gegevensbescherming, met de tweedeling tussen ‘derde pijler regels’ en communautaire regels, weinig transparant is? Zou het geen aanbeveling verdienen wanneer de Europese informatiesystemen onder één gemeenschappelijke kader van gegevensbescherming komen, waarbij deze algemene regels per sector of onderwerp kunnen worden uitgewerkt in meer specifieke regels?
- Kan de regering aangeven welk gevolg wordt gegeven aan het Griekse voorstel inzake uniforme regels voor gegevensbescherming in de derde pijler dat tijdens de JBZ Raad van juni 2003 is voorgelegd?

3. Doelbinding

- Deelt de regering de mening van de Permanente Commissie dat de naleving van het, voor gegevensbescherming belangrijke, doelbindingsbeginsel moeilijker te garanderen is, naarmate het informatiesyteem grootschaliger is en naarmate er meer staten en autoriteiten van gebruik maken?

- Kan de regering aangeven in hoeverre bovenstaand aspect bij de besluitvorming over Europese informatie systemen expliciet wordt meegewogen?

4. Opname gegevens

- Is de regering het er mee eens dat hoe ruimer het gebruik van de in de voorgestelde systemen opgenomen persoonsgegevens, en hoe meer autoriteiten hiertoe toegang hebben, des te strenger de eisen zullen moeten zijn met betrekking tot de adequaatheid en de juistheid van die gegevens?
- Kan de regering aangeven in hoeverre er voor wordt gezorgd dat grootschalige, multifunctionele informatiesystemen alleen zogenaamde 'harde gegevens' bevatten, dat wil zeggen informatie waarvan vooraf is getoetst dat die een werkelijke situatie of eigenschap weergeeft en welke informatie niet is gebaseerd op vermoedens of op het gebruik van zogenaamde profielen?
- Kan de regering aangeven of voor de toekomstige Europees informatiesystemen wordt gekozen voor een regeling met duidelijke, nauwkeurig omschreven criteria op grond waarvan personen in deze systemen worden opgenomen? Is de regering het ermee eens dat een dergelijke regeling de voorkeur verdient boven een regeling van wederzijdse erkenning van nationale besluiten om iemand in een systeem op te nemen?

5. Gebruikers – toegang aan derden

- Kan de regering er zorg voor dragen dat wanneer is vastgesteld welke nationale autoriteiten toegang krijgen tot een bepaald systeem, de lidstaten de lijsten met deze gebruikers aan hun nationale en het Europees parlement overleggen of anderszins openbaar maken?
- Kan de regering garanderen dat gegevensverstrekking aan derden uit de toekomstige Europese systemen, uitsluitend zal geschieden op basis van duidelijke, wettelijk geregelde criteria aan bepaalde vooraf vastgestelde instanties? Zal de regering er zorg voor dragen dat de besluitvorming hierover in een democratisch kader en in overleg met toezichtorganen voor de gegevensbescherming plaatsvindt?
- Is de regering het er mee eens dat de besluitvorming omtrent het gebruik van het SIS of het VIS, en de gegevensverstrekking daaruit, niet aan de discretionaire bevoegdheid van hetzij een agentschap die dit systeem beheert, noch aan de nationale overheden mag worden overgelaten?
- Wil de regering er zich voor inzetten dat aan toekomstige gegevensverstrekking aan derde staten strenge eisen worden gesteld, zoals: gegevensuitwisseling mag enkel plaatsvinden op basis van een concreet verzoek met toetsing door een toezichthoudend orgaan; de ontvangende staat moet de garantie bieden dat de gegevens voor een beperkt en concreet doel worden gebruikt; en het individu dient te worden geïnformeerd over de gegevensverstrekking aan derde staten of instanties? Deelt de regering de mening dat iedere afspraak over gegevensverstrekking aan derde staten op basis van wederkerigheid dient te geschieden?

6. Bewaartermijnen

- Kan de regering het parlement informeren over welke bewaartermijnen op dit moment worden voorgesteld bij de onderhandelingen over zowel SIS II als het VIS?
- Deelt de regering de mening dat, om het gebruik van verouderde, onbruikbare gegevens te voorkomen, per categorie gegevens en per doel waarvoor die gegevens worden opgeslagen, een passende bewaringstermijn moeten worden vastgesteld?

7. Individuele rechten

- Op welke wijze wordt in de regeling van de toekomstige informatiesystemen erin voorzien dat de burger zoveel mogelijk vooraf wordt geïnformeerd over het gebruik van zijn of haar gegevens? Kan de regering er zich voor inzetten dat de burger in ieder geval op het moment van afname van biometrische gegevens wordt ingelicht over doel, gebruik en rechten van de betrokkene?

- Wil de regering zich inzetten voor een regeling waarbij de betrokken persoon tijdig en volledig wordt geïnformeerd, waarbij de verstrekte informatie zowel duidelijkheid biedt over het voorgenomen doel van de gegevensopslag, wie de gebruikers zijn van die informatie, wat de bewaartermijnen zijn en ten slotte welke rechten en rechtsmiddelen de betreffende persoon heeft?

8. Effectieve rechtsmiddelen

- Kan de regering aangeven op welke wijze bij de toekomstige systemen als het SIS II en VIS, zorg wordt gedragen voor een eenvoudige en effectieve toegang tot de rechter? Zal de regeling van rechtsmiddelen gekozen worden voor het systeem van het huidige SIS, waarbij een individu zelf kan kiezen op welk grondgebied het een procedure wil starten? Zal het rechtsmiddel openstaan ten aanzien van zowel het besluit om iemand in een informatiesysteem op te nemen, als ten aanzien van het besluit dat op basis van een in een dergelijk systeem opgenomen informatie is genomen?
- In de huidige regeling van de Schengen Uitvoeringsovereenkomst is ervoor gekozen dat iedere uitspraak van een nationale rechter of toezichtinstantie in verband met de rechtmatigheid van gegevensverwerking, moeten worden nageleefd door de nationale autoriteiten van de andere Schengen staten. Zal deze regeling ook het uitgangspunt worden ten aanzien van SIS II en het toekomstige VIS?

9. Internationaal toezichtorgaan

- Is de regering het met de Permanente Commissie eens dat er op Europees niveau één orgaan moet worden ingesteld dat toezicht houdt op de persoonsinformatiesystemen die op basis van Europees recht zijn ingesteld en die door de nationale autoriteiten van de EU lidstaten worden gebruikt? Onderschrijft de regering het voorstel om dit Europees toezichtorgaan eventueel toe te rusten met gespecialiseerde kamers voor de afzonderlijke Europese informatiesystemen?
- Kan de regering er zorg voor dragen dat de Europese en nationale toezichtorganen voor de gegevensbescherming voldoende financiële middelen krijgen om hun taken naar behoren uit te kunnen voeren? Zullen deze organen ook worden toegerust met bindende instrumenten, zoals bijvoorbeeld de mogelijkheid een instantie te verplichten tot verwijdering of correctie van gegevens; de bevoegdheid boetes op te leggen; en te bevelen dat gegevensverwerking bij ernstige schending van de regelgeving wordt stopgezet?

10. Evaluatieplicht

- Wil de regering er zich voor inzetten dat in de wettelijke regeling van ieder toekomstig informatiesysteem een evaluatieplicht wordt opgenomen inzake het gebruik en de effecten van deze systemen? En dat zo een evaluatie moet worden uitgevoerd binnen een bepaalde termijn (bijvoorbeeld twee jaar) na het operationeel worden van het informatiesysteem? Deelt de regering de mening dat een dergelijke evaluatie de effecten wat betreft het gebruik, de behaalde doelen, de rechtsbescherming en de kosten moet bestrijken?