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
http://www.commissie-meijers.nl

Aan: De vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties
van de Tweede Kamer der Staten-Generaal

Betreft: Notitie over de mogelijke consequenties van aanhangige Europese voorstellen over de opzet van grootschalige gegevensbestanden en de uitwisseling van persoonsgegevens

Kenmerk: CM0605-I
Datum: 13 april 2006

Geachte leden van de Staten-Generaal,

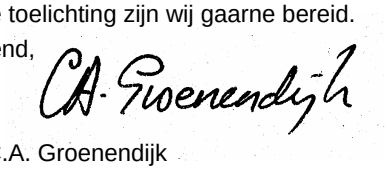
De Permanente Commissie vraagt uw aandacht voor verschillende, op dit moment in Brussel aanhangige, voorstellen inzake de opzet van grootschalige gegevensbestanden en de uitwisseling van persoonsgegevens. Deze voorstellen betreffen de opzet van een Visum Informatie Systeem (VIS), de vervanging van het huidige Schengen Informatiesysteem (SIS) door SIS II en het voorgestelde gebruik van biometrie in deze systemen en op reisdocumenten en paspoorten (zie het overzicht en de stand van zaken van de aanhangige voorstellen in bijlage 2 van deze brief). Daarnaast wijst de Permanente Commissie naar de inhoud van recente mededelingen van de Europese Commissie inzake het interoperabiliteitsbeginsel en het beginsel van beschikbaarheid van informatie ('*principle of availability*'). Volgens het eerste beginsel zullen het gebruik en de onderlinge samenhang van de verschillende systemen worden verruimd, op basis van het tweede beginsel zullen lidstaten in bepaalde situaties worden verplicht de in de nationale bestanden voorhanden persoonsinformatie ter beschikking stellen aan andere lidstaten.

De op grond van deze voorstellen te nemen maatregelen vormen naar het oordeel van onze commissie een aantasting van grondrechten zoals het recht op privé leven en het non-discriminatie beginsel. Daarnaast zijn de voorstellen in strijd met de kernbeginselen van het Europese recht inzake de gegevensbescherming, zoals het doelbindingsbeginsel en de bescherming van de rechten van geregistreerden. De registratie van persoonsgegevens van zowel EU als niet-EU onderdanen en de mogelijkheid om deze personen te controleren of zelfs de toegang tot het EU grondgebied te weigeren, is bovendien in strijd met het recht op vrij verkeer van EU onderdanen en legaal verblijvende derdelanders. Ten aanzien van het voorgestelde gebruik en de (centrale) opslag van biometrische gegevens, zijn de mogelijke voordelen en risico's nog onvoldoende in kaart gebracht. De Europese bewindslieden lijken daarbij geen acht te slaan op de kritische rapporten van onafhankelijke adviesorganen over dit onderwerp.

Het Europese Parlement en de nationale parlementen hebben onvoldoende zeggenschap over toekomstige systemen en het gebruik van technologie daarbij. Voor een duidelijk beeld van de consequenties van de voorstellen, dienen de huidige voorstellen in hun samenhang te worden gezien. Vóórdat ingestemd kan worden met de genoemde voorstellen, moeten minimumvoorwaarden ter bescherming van de betrokken individuen worden vastgesteld.

In 2003 heeft de Permanente Commissie in een uitgebreid commentaar al haar bezorgdheid uitgesproken naar aanleiding van deze Europese ontwikkelingen (CM0313, 20 november 2003). Met het oog op de komende besluitvorming en vanwege het belang van dit onderwerp worden in de bijgaande notitie (bijlage 1) de verschillende voorstellen nog eens kort besproken en van kanttekeningen voorzien. Bijlage 2 geeft een overzicht en de stand van zaken van de belangrijkste voorstellen.

Tot nadere toelichting zijn wij gaarne bereid.
Hoogachtend,



Prof. mr. C.A. Groenendijk
voorzitter

Bijlage 1 *Notitie van de Permanente Commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen- en strafrecht naar aanleiding van huidige ontwikkelingen in de EU inzake de opslag en uitwisseling van persoonsgegevens (gebruik van biometrie, invoering VIS en SIS II en de implementatie van de beginselen van interoperabiliteit en beschikbaarheid van informatie)*

1 Algemeen

Op EU niveau worden belangrijke besluiten voorbereid inzake de opzet van grootschalige bestanden met persoonsgegevens en inzake gegevensuitwisseling. Deze voorstellen betreffen onder meer de opzet van een Visum Informatie Systeem (VIS), de vervanging van het huidige Schengeninformatiesysteem (SIS) door SIS II en het voorgestelde gebruik van biometrie in deze systemen en op reisdocumenten en paspoorten. Daarnaast heeft de Europese Commissie eind 2005 twee mededelingen gepubliceerd waarin voorstellen worden gedaan voor het toekomstige beleid inzake het gebruik van persoonsinformatie. Centraal in deze mededelingen staan enerzijds het beginsel van interoperabiliteit en anderzijds het beginsel van beschikbaarheid van informatie (*'principle of availability'*). Op grond van het eerste beginsel wil de Europese Commissie het gebruik van en de onderlinge samenhang tussen de verschillende systemen vergroten, op basis van het tweede beginsel moeten lidstaten in bepaalde situaties verplicht worden de in de nationale bestanden voorhanden persoonsinformatie ter beschikking stellen aan andere lidstaten.
De noodzaak en proportionaliteit van de bovengenoemde voorstellen zijn slecht onderbouwd, terwijl de consequenties van deze maatregelen ingrijpend zijn. Op grond van de huidige plannen zullen verschillende systemen voor verschillende beleidsdoelen en door een groot aantal autoriteiten worden gebruikt. Per doel is niet vastgesteld of het opslaan en uitwisselen van persoonsgegevens daadwerkelijk voor dit doel effectief is, dan wel of de beoogde voordelen opwegen tegen de nadelen zoals de hoge kosten van de voorgestelde systemen en de inbreuk op de individuele rechten. Door de invoering van dergelijke grootschalige systemen gekoppeld aan het gebruik van biometrie, zullen ambtenaren bij hun besluiten steeds meer vertrouwen op de in deze systemen opgeslagen gegevens en de door die systemen uitgevoerde controles. Deze ontwikkelingen verkleinen de kans dat ambtenaren met mogelijke fouten in deze systemen rekening houden, dat zij controleren of de nationale besluiten tot registratie rechtmatig zijn, of dat zij in een concreet geval nog een individuele belangenafweging maken.

De verschillende maatregelen worden los van elkaar aan het parlement voorgelegd. De risico's en gevolgen voor de individuele rechten van personen van de voorgestelde systemen kunnen echter alleen goed in kaart worden gebracht wanneer de voorstellen in hun onderlinge samenhang worden beoordeeld. Besluiten die ten aanzien van het ene systeem worden genomen, hebben ook gevolgen voor het gebruik van andere systemen omdat systemen aan elkaar worden gekoppeld of omdat één autoriteit de toegang verkrijgt tot de verschillende systemen. In de volgende paragrafen volgt een kort overzicht van de belangrijkste ontwikkelingen. In paragraaf 7 formuleert de Permanente Commissie minimum voorwaarden die naar haar mening ten grondslag moeten liggen aan de besluitvorming.

2 SIS II

Het voorstel voor invoering van het SIS II (zie COM (2005) 236) beoogt niet alleen het gebruik van het huidige SIS uit te breiden naar alle 25 (en de mogelijke toekomstige) EU lidstaten, maar ook het gebruik en de toegankelijkheid van de opgeslagen gegevens te verruimen. Invoering van SIS II betekent niet alleen dat het aantal personen dat is opgenomen in dit systeem exponentieel zal toenemen, maar ook het aantal gebruikers. Met de gevolgen van een dergelijke massale opslag en uitwisseling van gegevens is onvoldoende rekening gehouden. Het is de vraag of de bewindslieden de ervaringen met het huidige SIS voldoende laten meewegen. Op basis van het huidige SIS kunnen niet-EU onderdanen de toegang worden geweigerd of worden uitgezet op basis van een niet door de weigerende of uitzettende staat te controleren besluit van een andere lidstaat (artikel 96 van de Schengen Uitvoeringsovereenkomst). Uit het inspectierapport van de Gemeenschappelijke Controle Autoriteit naar de toepassing van artikel 96 van 20 juni 2005, blijkt dat het aantal ten onrechte gesignaleerde personen in het SIS een groot probleem is: personen worden op grond van

onwettige criteria opgenomen, tijdslimieten worden niet in acht genomen en nog steeds worden EU onderdanen als te weigeren vreemdeling in het SIS geregistreerd.

- De betrokken regeringen hebben voor dit probleem van bestandsvervuiling geen concrete maatregelen voorgesteld, laat staan genomen. In het licht van de ervaringen met het huidige SIS zijn voorzorgsmaatregelen echter wel noodzakelijk en ook vóórdat SIS II in werking treedt.
- De toepassing van het huidige SIS, maar ook SIS II, waarbij een individu de toegang kan worden geweigerd of zelfs kan worden uitgezet op basis van een in dat SIS geregistreerd besluit van een andere lidstaat, is ook om twee meer principiëlere redenen problematisch. In de eerste plaats is een dergelijke toepassing van het SIS in strijd met het beginsel zoals neergelegd in artikel 15 lid 1 van de EG Richtlijn inzake de bescherming van persoonsgegevens (95/46). Dit artikel bepaalt dat *'eenieder het recht heeft niet te worden onderworpen aan een besluit waaraan rechtsgevolgen zijn verbonden en dat louter wordt genomen op grond van geautomatiseerde gegevensverwerking'.*
- Ten tweede kan een *'automatisch'* op basis van het SIS gebaseerde toegangsweigering ten aanzien van EU onderdanen en bepaalde groepen derdelanders in strijd zijn met hun recht op vrij verkeer. Dit is recent geconcludeerd in een uitspraak van 31 januari 2006 door het Hof van Justitie (C-503/03). In deze uitspraak veroordeelde het Hof een Spaans besluit waarin een Algerijnse echtgenoot van een Spaanse onderdaan de toegang was geweigerd op basis van een SIS signalering, als in strijd met het recht op vrij verkeer van personen.

3 VIS

In december 2004 presenteerde de Europese Commissie een voorstel voor een centraal systeem voor de opslag van gegevens over visumaanvragen: het Visum Informatie Systeem (het 'VIS'), COM (2004) 835. In dit systeem zullen niet alleen alle beslissingen waarbij een visum wordt verstrekt voor het EU grondgebied worden opgeslagen, maar ook alle beslissingen over geweigerde visumaanvragen en alle besluiten inzake intrekking of verlenging van een visum. Het VIS wordt een centraal databestand voor het hele EU grondgebied waarin jaarlijks miljoenen gegevens over individuen zullen worden opgenomen. Deze gegevens kunnen voor tenminste vijf jaar worden bewaard. In het VIS zullen niet alleen gegevens over visumplichtige derdelanders worden opgenomen, maar ook over EU onderdanen of Europese bedrijven die de betrokkenen uitnodigen of voor deze persoon garant staan. Ook is voorzien voor de opname van biometrische gegevens in het VIS. Vanaf het begin is dit systeem opgezet als een '*multifunctioneel instrument'.* De centrale opslag dient niet alleen voor de (snellere) afhandeling van visumaanvragen, maar wordt ook ingezet als middel tegen fraude en '*visa-shopping'*, voor de interne veiligheid en ter bestrijding van illegale immigratie en terrorisme. Zo moet bijvoorbeeld met het VIS de mogelijkheden voor de terugkeer van illegale immigranten worden verbeterd. In november 2005, is een voorstel voor een besluit gepubliceerd voor de verlening van toegang tot het VIS van interne veiligheidsdiensten van de lidstaten en Europol ter voorkoming, bestrijding en onderzoek van terroristische misdrijven en andere ernstige misdrijven (voorstel van 24 november 2005, COM (2005) 600).

Het bovenstaande betekent dat een groot aantal organen en autoriteiten van de 25 lidstaten toegang tot deze gegevens hebben, voor uiteenlopende taken. De Permanente Commissie zet grote vraagtekens bij het voorgestelde systeem. Het voorgestelde systeem zal aan zeer strenge voorwaarden moeten voldoen, wil men voorkomen dat op basis van dit systeem de rechten en belangen van de betrokken individuen op grote schaal worden geschonden. Belangrijke amendementen zijn daartoe voorgesteld in het ontwerp rapport van de rapporteur van het Europees Parlement Ludford van 8 november 2005 (2004/0287 (COD). Deze betreffen onder andere een duidelijker en meer afgebakende doelomschrijving van VIS, een duidelijkere informatieplicht aan de geregistreerden en een maximum tijdslimiet van vijf jaar voor de opslag van de gegevens. Ook heeft rapporteur Ludford terecht voorgesteld dat grensambtenaren enkel toegang mogen hebben tot biometrische gegevens zoals opgeslagen op de reisdocumenten zelf. Voor hun taak, verificatie van de identiteit van de betreffende persoon, is het niet nodig een centraal bestand met biometrische gegevens te raadplegen. Zij verwijst daarbij naar diverse rapporten van onafhankelijke adviesorganen waarin de centrale opslag van biometrie disproportioneel is genoemd en is afgewezen.

- De Permanente Commissie onderschrijft de voorstellen van rapporteur Ludford en hoopt dat zij door de Raad en de Commissie worden overgenomen. Zij raadt de Staten-Generaal aan de regering te vragen haar stem in de Raad voor dat doel te gebruiken.

- Daarnaast dient de regeling een sterke rechtsbescherming aan de betrokkenen te bieden. Dit houdt in: een recht op toegang tot de rechter, recht op schadevergoeding bij onjuist of misbruik van de opgeslagen gegevens, de bevoegdheid van rechters en toezichthoudende instanties om boetes op te leggen aan autoriteiten die het VIS voor oneigenlijke doeleinden gebruiken of die niet zorgdragen voor de juiste en volledige opslag van de persoonsgegevens in het VIS.

4 Invoering biometrie

De Permanente Commissie onderkent dat het gebruik van biometrie in databestanden en de opname in reisdocumenten voordelen kan opleveren, ook voor de betrokken individuen, nu hiermee foute identificatie (door slecht gespelde namen, dubbelgangers) kan afnemen en bepaalde procedures voor de betrokkene, zoals visumaanvragen sneller kunnen worden afgehandeld. De vraag is echter of deze mogelijke voordelen opwegen tegen de mogelijke risico's verbonden aan het gebruik van biometrie. Op dit moment zijn er nog te veel onbeantwoorde vragen over de betrouwbaarheid van biometrie en de over de consequenties van verschillende opslagtechnieken. Welke techniek geeft geen (of aanvaardbaar klein) risico van foute identificatie? De Permanente Commissie, onder verwijzing naar een eerder advies inzake het VIS van de Europese Toezichthouder voor Data Protectie Protectie (European Data Protection Supervisor, EDPS), heeft er al eerder op gewezen dat bijvoorbeeld bij een systeem als het VIS waar naar verwachting gegevens over meer dan 20 miljoen personen per jaar zullen worden opgeslagen, een *'False Rejection Rate*' van bijvoorbeeld 0,5 tot 1 % zou betekenen dat 100 tot 200.000 personen ten onrechte niet zouden worden herkend: betekent dit dan dat zij automatisch geen visum krijgen of aan hen toegang wordt geweigerd? Welke techniek is het minst 'ingrijpend' voor betrokkenen? Welke oplossingen worden geboden aan die personen die om fysieke of andere gronden niet geschikt zijn voor biometrische herkenning? De Permanente Commissie wijst erop dat in verschillende brieven en reacties van nationale en Europese data protectie autoriteiten ook afwijzend is gereageerd op voorstellen voor centrale opslag van biometrische gegevens. In zijn advies over de mededeling van de Commissie inzake interoperabiliteit van 10 maart 2006, wijst de EDPS op de ongeschiktheid van biometrie als *'primary key'* zoals voorgesteld door de Commissie om gegevens uit verschillende systemen met elkaar te vergelijken. Omdat biometrische kenmerken altijd uitgaan van waarschijnlijkheden zijn zij niet geschikt als ondubbelzinnige sleutel voor de vaststelling van iemands identiteit, aldus de Europese Toezichthouder. In de huidige besluitvorming worden deze adviezen echter genegeerd door de Europese bewindslieden. Ook wordt onvoldoende nagedacht over de optie om biometrische gegevens niet op te slaan in een database maar slechts ter verificatie of identificatie te gebruiken (bv. alleen op paspoort of ID opslaan). Bij een dergelijke keuze moet worden uitgesloten dat onbevoegden toegang krijgen tot de op de identiteitskaart of paspoort opgeslagen gegevens. Ook moet worden gelet op het risico dat buitenstaanders de opgeslagen gegevens wijzigen. In de zomer van vorig jaar werd door een onderzoeksteam in Delft vastgesteld dat gegevens, opgeslagen op een chip volgens een techniek die zowel door de Britse als de Nederlandse regering was voorzien voor gebruik voor het nationaal paspoort, door derden via speciale afleesapparatuur op afstand konden worden 'meegelezen'.

- Dergelijke onderzoeken maken duidelijk dat bewindslieden hun keuzes voor bepaalde technieken moeten onderbouwen en de gevolgen van deze keuzes volledig in kaart moeten brengen. Bij de keuze van biometrie voor identificatie doeleinden moet men die techniek kiezen die het betrouwbaarst is.
- Voorkomen moet worden dat personen ten onrechte niet worden herkend en daardoor toegang of voorzieningen worden geweigerd of dat personen ten onrechte wel worden 'herkend' en daarmee door de mazen van het (opsporings-)systeem glippen.

5 Principe van beschikbaarheid

Het beginsel van beschikbaarheid van informatie of '*exchange of information under the principle of availability'* is door de Europese Commissie voorgesteld als basisbeginsel voor de toekomstige samenwerking tussen de autoriteiten van de verschillende EU lidstaten (zie het voorstel voor een kaderbesluit, 12 oktober 2005, COM (2005) 490). Met dit beginsel wil de Europese Commissie nationale autoriteiten verplichten om de, bij die autoriteiten aanwezige informatie, uit te wisselen met andere buitenlandse autoriteiten, zonder dat hieraan

een individuele belangenafweging vooraf gaat. De Europese Commissie gaat uit van het beginsel: aanwezige informatie is beschikbare informatie. Dit voorgestelde principe is in eerste instantie bedoeld ter verbetering van de samenwerking tussen opsporingsinstanties, ter opsporing en vervolging van strafbare feiten.
In de politieke discussie wordt het beginsel van beschikbaarheid van informatie een veel ruimere betekenis toegemeten. Op dit moment circuleren bijvoorbeeld voorstellen om Eurodac (de databank met vingerafdrukken van asielzoekers) te gebruiken voor opsporingsdoeleinden, om nationale veiligheidsdiensten toegang te verlenen tot VIS en om verschillende EU bestanden open te stellen voor gebruik door derde staten waaronder Verenigde Staten en Canada (zie het rapport *'Friends of the Presidency on the technical modalities to implement the principle of availability'*, 10 November 2005, Raadsdoc. 13558/1, p.15).
Parallel aan deze ontwikkelingen loopt de ondertekening en ratificatie van het intergouvernementele Verdrag van Prüm (Trb. 2005, 197). Met dit verdrag wordt buiten EU kader om al een voorproef genomen op het beginsel van beschikbaarheid van informatie door de autoriteiten van de ondertekenende lidstaten direct toegang te geven tot elkaar gegevensbestanden.

- Ten aanzien van al deze voorstellen onderstreept de Permanente Commissie nog eens haar centrale bezwaar, namelijk dat er onvoldoende aandacht is voor enerzijds de noodzaak voor de (verplichte) gegevensuitwisseling en anderzijds de risico's voor informatievervuiling en aantasting van de rechten van betrokken burgers.

6 Principe van interoperabiliteit

In de zienswijze van de Europese Commissie moet het beschikbaarheidsprincipe aangevuld worden met het beginsel van de *'interoperabiliteit'* (zie de Mededeling inzake de verbetering van de doeltreffendheid, de interoperabiliteit en de synergie van Europese gegevensbanken van de Commissie van 24 november 2005, COM (2005) 597). Interoperabiliteit wordt anders dan in wetenschappelijke literatuur voorgesteld als een louter technisch, niet-politiek concept dat beoogt om *'beschikbare gegevens beter te gebruiken onder meer door uitwisseling en interconnectie'*. Waar een dergelijk beginsel binnen de sfeer van politie en justitie als acceptabel en wenselijk mag worden beschouwd, gaat de Europese Commissie in de Mededeling onmiddellijk over tot de bespreking van verdergaande scenario's waarin, enerzijds, justitie en politie toegang krijgen tot alle bestaande EU-databanken en waarbij bij voorkeur gebruik wordt gemaakt van toegangsleutels tot systemen zoals biometrie en unieke nummers en waarin, anderzijds, inlichtingendiensten en veiligheidsdiensten ook toegang krijgen tot de genoemde systemen. Omdat de Europese Commissie beseft dat deze scenario's politiek gevoelig liggen, hoewel het om een 'technisch' onderwerp gaat, wordt alvast voorgesteld om alle EU systemen een zelfde technisch platform te geven waardoor interoperabiliteit alleszins op technisch vlak een feit is. Juridisch niet-bindende documenten zoals de Mededeling van de Commissie over interoperabiliteit blijken in de praktijk van Europa erg belangrijke drijfveren voor verdere besluitvorming te zijn. Alleen al de publicatie ervan is een belangrijk politiek feit. Meerdere auteurs, waaronder de Voorzitter van het Nederlands College Bescherming Persoonsgegevens hebben gewezen op het eenzijdig veiligheidsdenken achter dergelijke initiatieven: 'more is better'. In de praktijk blijkt evenwel dat de benodigde informatie al beschikbaar is, maar dat deze wegens verkeerde prioriteitstelling niet adequaat wordt gebruikt. Culturele en organisatorische componenten die informatiebeheer tot een succes kunnen maken, worden in de Commissiedocumenten onvoldoende gethematiseerd. In dit licht is het uitgangspunt dat het opzetten van een informatiestructuur met veel informatieregistraties 'achteraf handig is', een bewijs van onmacht.

- Afgezien van de vraag of de uitbreiding van het gebruik van de huidige systemen daadwerkelijk noodzakelijk en efficiënt is, zijn aan deze uitbreiding ook nog andere risico's verbonden. De voorgestelde uitbreiding van toegang tot systemen als Eurodac, SIS II en VIS door talrijke andere instanties (met inbegrip van derde landen) is zorgwekkend, in de eerste plaats omdat hiermee het oorspronkelijke doel van deze systemen wordt gewijzigd ('*function creep*').
- Ook leidt een dergelijk omvangrijk gebruik van gegevens, er toe dat vervuilde of onjuiste gegevens terechtkomen bij talrijke andere overheidsinstanties. Een grootschalig en ruim gebruik van persoonsgegevens stelt hoge eisen aan de betrouwbaarheid en juistheid van die gegevens. Zoals hierboven aangegeven, worden deze eisen op dit moment met het huidige SIS nog niet waargemaakt.

7 Minimum voorwaarden

De uitwisseling van persoonsgegevens en de opzet en beheer van centrale databestanden op Europees niveau moeten aan strenge voorwaarden worden gebonden. Wanneer deze voorwaarden niet op EU niveau worden gerealiseerd, dient de nationale wetgever er zich van bewust te zijn dat er nog ‘een tweede kans’ is: namelijk de implementatie van de Europese voorstellen. Ook in de nationale wetgeving kunnen belangrijke waarborgen worden ingebouwd ter bescherming van het individu en ter voorkoming dat nationale instanties geen controle meer kunnen uitoefenen op persoonsgegevens die zijzelf hebben verzameld.

Minimum voorwaarden die tenminste in acht moeten worden genomen zijn:

1) alleen verzamelen en opslaan van persoonsgegevens voor expliciet wettelijk omschreven doelen en alleen wanneer dit noodzakelijk en proportioneel is met het oog op dat beoogde doel;

2) geen centrale opslag van biometrische gegevens, noch op nationaal als internationaal niveau;

3) voor de opslag van bijzondere categorieën gegevens zoals genoemd in art. 8 EG Richtlijn 95/46 inzake de bescherming van persoonsgegevens moeten bijzondere waarborgen gelden ter voorkoming van ongelijke behandeling;

4) gegevensuitwisseling op grond waarvan nationale overheden elkaar nationale administratieve besluiten erkennen en uitvoering geven, dient vooraf te worden gegaan door harmonisatie van de criteria voor de betreffende besluitvorming;

5) betrokkenen moeten vooraf worden geïnformeerd over het doel van de opslag van zijn of haar gegevens.

6) besluiten die worden genomen op basis van opgeslagen informatie moeten worden gemotiveerd, ook moet worden aangegeven welke staat en welke autoriteit van deze staat de gegevens in het betreffende systeem heeft opgenomen;

7) korte limieten voor opslag gegevens, bij niet naleving moet de mogelijkheid bestaan voor rechters of data protectie autoriteiten om sancties op te leggen voor de betreffende autoriteiten;

8) geen toegang voor derde landen tot persoonsgegevens opgeslagen in EU bestanden zonder uitgebreide en expliciete rechtswaarborgen voor individuen.

9) expliciet recht op toegang tot de rechter voor iedereen die met het gebruik of negatieve besluitvorming op basis van de genoemde databestanden wordt geconfronteerd;

10) uitbreiding van bevoegdheden en faciliteiten voor nationale rechters en toezichtorganen. Deze instanties dienen tenminste te worden toegerust met de bevoegdheid van blokkering van verdere gegevensverwerking en het opleggen van boetes of het toekennen van schadevergoeding. Ook moeten zij de bevoegdheid hebben om de rechtmatigheid te toetsen van het besluit dat ten grondslag ligt aan opname gegevens, ook indien dat besluit door autoriteit van andere lidstaat is genomen.

Literatuur:

Working Document on biometrics of the Article 29 Data Protection Working Group on biometrics, 1 August 2003, WP 80 http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup

Opinion of the European Data Protection Supervisor (EDPS) on the proposal for VIS, 23 March 2004 www.edps.eu.int

Opinion of the European Data Protection Supervisor (EDPS) on the proposals for SIS II (the second-generation Schengen Information System, 19 October 2005.

Opinion of the European Data Protection Supervisor (EDPS) on the proposal for a regulation concerning the Visa Information System, 20 January 2006

Opinion the European Data Protection Supervisor (EDPS) on the proposal for a Council Framework Decision on principle of availability, 28 February 2006

Comments of the European Data Protection Supervisor (EDPS) on the Communication of the Commission on the interoperability of European databases, 10 March 2006

Opinion of the Article 29 Working Party on Data Protection on Regulation 2252/2004 on biometrics in passports and travel documents, 30 September 2005

Report of the Schengen Joint Supervisory Schengen Authority on an inspection on the use of Article 96 alerts in the Schengen Information System, Brussels, 20 June 2005, gepubliceerd op www.statewatch.org.

Progress report on application of the principles of Convention 108 on the collection and processing of biometric data, Consultative Committee of the Convention for the Protection of Individuals with regard automatic processing of personal data, the Council of Europe, February 2005, T-PD (2005) BIOM E.

Thierry Balzacq, Didier Bigo, Sergio Carrera and Elspeth Guild (2006)*, Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats*, 2006, Ceps Working Paper no. 234, 28p. Available at: www.ceps.be

Evelien Brouwer, *Data surveillance and border control in the EU: Balancing efficiency and legal protection of third country nationals* http://www.libertysecurity.org/article289.html

Paul De Hert, 'What are the risks and what guarantees need to be put in place in view of interoperability of police databases?' *Standard Briefing Note 'JHA & Data Protection*, No. 1: (14pages produced in January 2006 on behalf of the European Parliament, available via http://www.vub.ac.be/LSTS

Bart Jacobs, Select before you Collect, *Ars Aequi* 54 (2005) 12, p. 106-109.

Jacob Kohnstamm, 'Geef privacy niet zomaar op voor terreur', *NRC-Handelsblad*, 19 August 2005, 7

Permanente Commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen- en strafrecht *Commentaar inzake de huidige voorstellen inzake het gebruik van Europese informatiesystemen (VIS, SIS II, biometrie)* **CM0313**, 20 November 2003

Bijlage 2 *Overzicht aanhangige Europese wetgevingsvoorstellen inzake de opslag en uitwisseling van persoonsgegevens (VIS, SIS II en de implementatie van de beginselen van interoperabiliteit en beschikbaarheid van informatie)*

Op dit moment zijn vijf voorstellen voor nieuwe Europese wetgeving aanhangig als mede een mededeling over enkele uitgangspunten voor gegevensuitwisseling. Hieronder wordt voor elk van deze voorstellen de stand van zaken aangeduid.

1. Voorstel van de Commissie van 28 december 2004 voor een *Verordening inzake het Visuminformatiesysteem (VIS)* COM (2004) 835. Codecisie procedure, stemming EP verwacht juli 2006, ontwerp rapport rapporteur Baroness Sarah Ludford, 8 november 2005, 2004/0287 (COD). Bespreking verwacht op JBZ-Raad 27 april 2006.

2. Voorstel voor ee*n besluit van de Raad over de toegang tot het informatiesysteem (VIS) voor raadpleging door nationale veiligheidsdiensten van de lidstaten en Europol, met het oog op het voorkomen, opsporen en onderzoeken van terroristische misdrijven en andere ernstige misdrijven*. 30 november 2005, COM (2005) 600, consultatie procedure, rapporteur Baroness Sarah Ludford, bespreking verwacht op JBZ Raad 27 april 2006.

3. Voorstel voor een *Verordening inzake SIS II*, COM (2005) 236, co-decisie procedure, rapporteur Coelho. Geamendeerd voorstel voor verordening inzake SIS II Oostenrijks voorzitterschap, Raadsdoc. 5709/06 van 27 januari 2006, behandeling verwacht in JBZ Raad 27 april 2006.

4. Voorstel voor een *Kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van politiële en justitiële samenwerking in strafzaken*, 11 oktober 2005, COM (2005) 475. Consultatie procedure, rapporteur Martine Roure. Debat in JBZ Raad verwacht op 27 april 2006 of 1 juni 2006.

5. Voorstel voor een *Kaderbesluit van de Raad betreffende de uitwisseling van informatie volgens het beschikbaarheidsbeginsel*, 12 oktober 2005, COM (205) 490. Consultatie procedure, rapporteur LIBE: Antoine Duquesne. Debat in JBZ Raad verwacht 27 april 2006.

6. *Mededeling van de Commissie over de verbetering van de doeltreffendheid, de interoperabiliteit en de synergie van Europese gegevensbanken op het gebied van Justitie en Binnenlandse Zaken*, 24 november 2005, COM (2005) 597.