EUROPESE COMMISSIE

Brussel, 20.7.2010

COM(2010)385 definitief

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

Overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

Overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht

1. INLEIDING

De Europese Unie heeft een lange weg afgelegd sinds de leiders van vijf Europese landen in 1985 in Schengen overeenkwamen de controles aan hun gemeenschappelijke grenzen af te schaffen. Uit hun afspraken kwam in 1990 de Schengenuitvoeringsovereenkomst voort, waarin een groot deel van het huidige informatiebeheerbeleid al in de kiem aanwezig was. De afschaffing van de controles aan de binnengrenzen had tot gevolg dat in hoog tempo een reeks maatregelen aan de buitengrenzen werd genomen, voornamelijk met betrekking tot de afgifte van visa, de coördinatie van het asiel- en immigratiebeleid, en de intensivering van de politiële, justitiële en douanesamenwerking in de strijd tegen grensoverschrijdende criminaliteit. Het Schengengebied en de interne markt zouden niet kunnen functioneren zonder grensoverschrijdende informatie-uitwisseling.

De terreuraanslagen in de Verenigde Staten in 2001 en de bomaanslagen in Madrid en Londen in 2004 en 2005 brachten een nieuwe dynamiek op gang in de ontwikkeling van het Europese informatiebeheer. De Raad en het Europees Parlement stelden in 2006 de richtlijn gegevensbewaring vast, met de bedoeling de nationale autoriteiten in staat te stellen bij de bestrijding van ernstige criminaliteit gebruik te maken van opgeslagen telecommunicatieverkeer- en locatiegegevens[1]. Vervolgens volgde de Raad het Zweedse initiatief om de grensoverschrijdende uitwisseling van gegevens in strafrechtelijke onderzoeken en inlichtingenoperaties te vereenvoudigen. In 2008 werd het Prümbesluit goedgekeurd om vaart te zetten achter de uitwisseling van DNA-profielen, vingerafdrukken en gegevens uit kentekenregisters bij de bestrijding van terrorisme en andere vormen van criminaliteit. Ook grensoverschrijdende samenwerking tussen financiële inlichtingeneenheden, bureaus voor de ontneming van vermogensbestanddelen, cybercriminaliteitplatforms, alsmede het inzetten van Europol en Eurojust door de lidstaten, worden als instrument in de strijd tegen ernstige criminaliteit gebruikt in het Schengengebied.

In de nasleep van de terreuraanslagen van 11 september 2001 voerde de Amerikaanse regering het Programma voor het traceren van terrorismefinanciering in (Terrorist Finance Tracking Program, TFTP) om vergelijkbare plannen te verijdelen door verdachte financiële transacties in de gaten te houden. Het Europees Parlement heeft onlangs ingestemd met de sluiting van de overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika

[1] Er bestaat nog geen geharmoniseerde EU-definitie van "ernstige criminaliteit". In het besluit van de Raad dat Europol toegang geeft tot het VIS (Besluit 2008/633/JBZ van de Raad, PB L 218 van 13.8.2008, blz.129) worden "ernstige strafbare feiten" gedefinieerd als de feiten die staan vermeld in het Europees aanhoudingsbevel (Besluit 2002/584/JBZ van de Raad, PB L 190 van 18.7.2002, blz.1). De richtlijn gegevensbewaring (Richtlijn 2002/58/EG, PB L 105 van 13.4.2006, blz. 54) laat de definitie van "ernstige criminaliteit" over aan de lidstaten. Het Europol-besluit (Besluit 2009/371/JBZ van de Raad, PB L 121 van 15.5.2009, blz. 37) bevat ook een lijst van strafbare feiten die als "ernstige criminaliteit" worden gedefinieerd; deze lijst is grotendeels vergelijkbaar maar niet identiek met de lijst in het besluit betreffende het Europees aanhoudingsbevel.

inzake de verwerking en doorgifte van gegevens betreffende het financiële berichtenverkeer van de Europese Unie naar de Verenigde Staten ten behoeve van het Programma voor het traceren van terrorismefinanciering (EU-VS TFTP-overeenkomst)[2]. De uitwisseling van persoonsgegevens van passagiers (Passenger Name Records, PNR) met derde landen heeft de EU ook geholpen terrorisme en andere vormen van ernstige criminaliteit te bestrijden[3]. De Commissie heeft nu PNR-overeenkomsten gesloten met de VS, Australië en Canada, en sinds kort buigt zij zich opnieuw over een PNR-systeem in de EU en het uitwisselen van dergelijke gegevens met derde landen.

De hierboven genoemde instrumenten hebben het vrije verkeer in het Schengengebied mogelijk gemaakt, bijgedragen aan het voorkomen en bestrijden van terreuraanslagen en andere uitingen van ernstige criminaliteit, en de ontwikkeling van een gemeenschappelijk visum- en asielbeleid bespoedigd.

In deze mededeling wordt voor het eerst een volledig overzicht gegeven van alle EU-maatregelen op het gebied van de verzameling, de opslag en de grensoverschrijdende uitwisseling van persoonsgegevens met het oog op rechtshandhaving en migratiebeheer die al zijn ingevoerd, die nu worden ingevoerd of waarover wordt gesproken. Burgers hebben het recht te weten welke persoonsgegevens van hen worden verwerkt en uitgewisseld, door wie dat gebeurt en waarom. Dit document biedt een transparant antwoord op die vragen. Het beschrijft het belangrijkste doel van deze instrumenten, de structuur, de soorten persoonsgegevens die worden verwerkt, de lijst van autoriteiten die toegang hebben tot de gegevens en de bepalingen die de gegevensbescherming en –bewaring regelen. Daarnaast bevat het document een beperkt aantal voorbeelden dat laat zien hoe deze instrumenten in de praktijk werken (zie bijlage I). Ten slotte schetst deze mededeling de basisbeginselen die ten grondslag moeten liggen aan het ontwerp en de evaluatie van instrumenten voor informatiebeheer op het gebied van vrijheid, veiligheid en recht.

Met een overzicht van EU-maatregelen die het beheer van persoonsgegevens regelen en een voorstel voor een reeks beginselen voor de ontwikkeling en evaluatie van dergelijke maatregelen, levert deze mededeling een bijdrage aan een beleidsdialoog tussen goed geïnformeerde belanghebbenden. Tegelijkertijd biedt zij een eerste aanzet tot een coherentere aanpak van de uitwisseling van persoonsgegevens voor rechtshandhavingsdoeleinden, een wens van de lidstaten waarop onlangs ook werd ingespeeld met de EU-strategie voor het beheer van rechtshandhavingsinformatie[4], en aanknopingspunten voor een gedachtewisseling over de vraag of er een Europees model voor informatie-uitwisseling moet komen op basis van een evaluatie van de bestaande informatie-uitwisselingsmechanismen[5].

---

2 Resolutie van het Europees Parlement, P7-TA-PROV(2010)0279 van 8.7.2010.

3 In tegenstelling tot "ernstige criminaliteit", zijn "terroristische misdrijven" duidelijk gedefinieerd in het Kaderbesluit van de Raad inzake terrorismebestrijding (Kaderbesluit 2002/475/JBZ, PB L 164 van 22.6.2002, blz. 3; gewijzigd bij Kaderbesluit 2008/919/JBZ van de Raad, PB L 330 van 9.12.2008, blz. 21).

4 Conclusies van de Raad over een strategie voor het beheer van rechtshandhavingsinformatie voor interne veiligheid in de EU; Raad Justitie en Binnenlandse Zaken, 30.11.2009; Vrijheid, veiligheid, privacy – Het Europees binnenlandsezakenbeleid in een open wereld, Rapportering van de informele adviesgroep op hoog niveau toekomst van het Europees binnenlandsezakenbeleid ("de Toekomstgroep"), juni 2008.

5 Het programma van Stockholm - Een open en veilig Europa ten dienste en ter bescherming van de burger, Raadsdocument 5731/10 van 3.3.2010, punt 4.2.2.

Doelbinding is een kernelement van alle instrumenten waarop deze mededeling betrekking heeft. De hoogste graad van informatie-uitwisseling zou worden bereikt met één enkel, overkoepelend EU-informatiesysteem dat voor verschillende doeleinden wordt gebruikt. Het invoeren van een dergelijk systeem zou echter een grove en onrechtmatige beperking vormen van het recht van personen op privacy- en gegevensbescherming, en de ontwikkeling en de werking ervan zouden enorme problemen opleveren. In de praktijk heeft het beleid op het gebied van vrijheid, veiligheid en recht zich snel ontwikkeld en een aantal informatiesystemen en –instrumenten van verschillende omvang en strekking en met verschillende doelen opgeleverd. De gecompartimenteerde structuur van het informatiebeheer die is ontstaan in de afgelopen decennia is bevorderlijker voor de bewaking van het recht op privacy van de burgers dan welk gecentraliseerd alternatief dan ook.

Deze mededeling gaat niet in op maatregelen die betrekking hebben op de uitwisseling van andere dan persoonsgegevens voor strategische doeleinden, zoals algemene risicoanalyses of dreigingsbeoordelingen; evenmin wordt er een uitvoerige analyse gemaakt van de gegevensbeschermingsbepalingen van de instrumenten die worden besproken, omdat de Commissie momenteel op basis van artikel 16 van het Verdrag betreffende de werking van de Europese Unie al werkt aan een nieuw algemeen kader voor de bescherming van persoonsgegevens in de EU. De Raad buigt zich op dit moment over ontwerp-onderhandelingsrichtsnoeren voor een overeenkomst tussen de EU en de VS over de bescherming van persoonsgegevens die worden doorgegeven en verwerkt met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, waaronder terrorisme, in het kader van politiële en justitiële samenwerking in strafzaken. Aangezien die onderhandelingen eerder zijn bedoeld om vast te stellen op welke manier beide partijen een hoog niveau van bescherming van de fundamentele rechten en vrijheden kunnen garanderen bij de doorgifte en verwerking van persoonsgegevens dan dat deze doorgifte en verwerking inhoudelijk moeten worden geregeld, heeft deze mededeling geen betrekking op dit initiatief[6].

2. EU-INSTRUMENTEN DIE DE VERZAMELING, DE OPSLAG OF DE UITWISSELING VAN PERSOONSGEGEVENS VOOR RECHTSHANDHAVINGS- OF MIGRATIEDOELEINDEN REGELEN

Dit onderdeel geeft een overzicht van de instrumenten van de Europese Unie die de verzameling, de opslag of de grensoverschrijdende uitwisseling van persoonsgegevens met het oog op rechtshandhaving of migratiebeheer regelen. Punt 2.1 heeft betrekking op maatregelen die al van kracht zijn, die nu worden ingevoerd of waarover nu wordt gesproken. Punt 2.2 gaat over maatregelen uit het actieplan ter uitvoering van het programma van Stockholm[7]. Elk punt geeft informatie over de volgende aspecten van ieder instrument:

– achtergrond (of de maatregel door de lidstaten werd voorgesteld of door de Commissie);[8]

---

6 COM(2010)252 van 26.5.2010.

7 COM(2010)171 van 20.4.2010 (Actieplan ter uitvoering van het programma van Stockholm).

8 In de voormalige derde pijler van de Europese Unie deelden de Commissie en de lidstaten het initiatiefrecht op het gebied van politiële en justitiële samenwerking in strafzaken. Bij het Verdrag van Amsterdam werden het beheer van de buitengrenzen, asiel en immigratie ondergebracht bij de communautaire (eerste) pijler, waarin de Commissie als enige het initiatiefrecht had. Het Verdrag van Lissabon heeft een einde gemaakt aan de pijlerstructuur van de Unie, maar het initiatiefrecht berust nog steeds bij de Commissie. Op het gebied van de politiële en justitiële samenwerking in strafzaken (met

– doel(en) waarvoor gegevens worden verzameld, opgeslagen of uitgewisseld;

– structuur (gecentraliseerd informatiesysteem of gedecentraliseerde gegevensuitwisseling);

– welke persoonsgegevens worden verzameld;

– autoriteiten die toegang hebben tot de gegevens;

– gegevensbeschermingsbepalingen;

– regels voor de bewaring van de gegevens;

– stand van uitvoering;

– evaluatiemechanisme.

2.1. Instrumenten die al worden gebruikt, die nu worden ingevoerd of waarover nu wordt gesproken

EU-instrumenten ter bevordering van de goede werking van het Schengengebied en de douane-unie

Het **Schengeninformatiesysteem** (SIS) is ontstaan uit de wens van de lidstaten om een gebied zonder controles aan de binnengrenzen te creëren en tegelijkertijd het verkeer van personen over de buitengrenzen te vergemakkelijken[9]. Het SIS is in 1995 in gebruik genomen en is bedoeld om de openbare veiligheid, waaronder de nationale veiligheid, in het Schengengebied te handhaven en het personenverkeer te vergemakkelijken met behulp van de informatie die via dit systeem wordt doorgegeven. Het SIS is een gecentraliseerd informatiesysteem met een nationaal deel in elk van de deelnemende lidstaten en een technisch ondersteunende functie in Frankrijk. De lidstaten kunnen signaleringen opnemen voor personen die met het oog op aanhouding voor uitlevering worden gezocht, onderdanen van derde landen die niet mogen worden toegelaten, vermiste personen, getuigen of personen die zijn gedagvaard, personen en voertuigen die onder bijzonder toezicht worden geplaatst omdat zij een bedreiging vormen voor de openbare of de nationale veiligheid, verdwenen of gestolen voertuigen, documenten en vuurwapens, en verdachte bankbiljetten. Bij de gegevens die in het SIS worden ingevoerd, gaat het om namen en aliassen, geboorteplaats en –datum, nationaliteit, en of de betrokkene gewapend en/of gewelddadig is. Politie, grenswacht, douane en gerechtelijke autoriteiten hebben in strafzaken toegang tot deze gegevens binnen de grenzen van hun respectieve bevoegdheden. Immigratieautoriteiten en consulaire posten hebben toegang tot de gegevens over onderdanen van derde landen die op de lijst van personen met een inreisverbod staan en tot de signaleringen betreffende verdwenen of gestolen documenten. Europol heeft toegang tot sommige categorieën SIS-gegevens, zoals signaleringen van personen die met het oog op aanhouding voor uitlevering worden gezocht, en die van personen die onder bijzonder toezicht worden geplaatst omdat zij een bedreiging vormen voor de openbare of de nationale veiligheid. Eurojust heeft toegang tot de

---

inbegrip van administratieve samenwerking), kan nog steeds wetgeving worden voorgesteld op initiatief van een kwart van de lidstaten.

[9] Overeenkomst ter uitvoering van het te Schengen gesloten akkoord van 14 juni 1985 tussen de regeringen van de staten van de Benelux Economische Unie, de Bondsrepubliek Duitsland en de Franse Republiek, betreffende de geleidelijke afschaffing van de controles aan de gemeenschappelijke grenzen (PB L 239 van 22.9.2000, blz. 19).

signaleringen van personen die met het oog op aanhouding voor uitlevering worden gezocht en tot die van personen die zijn gedagvaard. Persoonsgegevens mogen alleen worden gebruikt voor het doel van de signalering waarvoor ze werden verstrekt. De persoonsgegevens die in SIS worden ingevoerd met het oog op de opsporing van personen mogen slechts worden bewaard zolang dat nodig is om het doel waarvoor ze werden verstrekt, te bereiken, maar in geen geval langer dan drie jaar. Gegevens over personen die onder bijzonder toezicht worden geplaatst omdat zij een bedreiging vormen voor de openbare of de nationale veiligheid moeten na een jaar worden verwijderd. De lidstaten moeten regels opstellen die een gegevensbeschermingsniveau garanderen dat ten minste gelijk is aan het niveau dat voortvloeit uit het Verdrag van de Raad van Europa uit 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens en de aanbeveling van het Comité van Ministers van de Raad van Europa tot regeling van het gebruik van persoonsgegevens op politieel gebied, uit 1987[10]. Hoewel de Schengenuitvoeringsovereenkomst geen evaluatieclausule bevat, kunnen de overeenkomstsluitende partijen wel wijzigingen van de overeenkomst voorstellen, die unaniem moeten worden goedgekeurd en moeten worden geratificeerd door de nationale parlementen. Het SIS is volledig in gebruik genomen in 22 lidstaten en in Zwitserland, Noorwegen en IJsland. Het Verenigd Koninkrijk en Ierland nemen deel aan de politiesamenwerking in het kader van de Schengenuitvoeringsovereenkomst en aan het SIS, behalve als het gaat om signaleringen van onderdanen van derde landen met een inreisverbod. Cyprus heeft de Schengenuitvoeringsovereenkomst wel ondertekend, maar is nog niet begonnen met de uitvoering. In Liechtenstein wordt de overeenkomst in 2010 van kracht, in Bulgarije en Roemenië waarschijnlijk in 2011. Zoeken in het SIS levert een treffer op als de gegevens van een gezochte persoon of een gezocht voorwerp overeenkomen met die van een bestaande signalering. Als het zoeken een treffer oplevert, kunnen rechtshandhavingsautoriteiten via hun netwerk van Sirene-bureaus aanvullende informatie opvragen over de gesignaleerde persoon of het gesignaleerde voorwerp[11].

Met de toetreding van nieuwe lidstaten tot het Schengengebied is de omvang van de SIS-database ook toegenomen: tussen januari 2008 en 2010 is het aantal SIS-signaleringen gestegen van 22,9 tot 31,6 miljoen[12]. De lidstaten zagen de toename van het aantal gegevens en de veranderingen in de gebruikersbehoeften aankomen en hebben in 2001 de Commissie opdracht gegeven een **Schengeninformatiesysteem van de tweede generatie** (SIS II) te ontwikkelen[13]. SIS II is momenteel in ontwikkeling en moet een hoog veiligheidsniveau garanderen in de ruimte van vrijheid, veiligheid en recht aan de hand van een verbeterde versie van de functies van het systeem van de eerste generatie; tevens moet SIS II het personenverkeer vergemakkelijken met behulp van de informatie die via dit systeem wordt doorgegeven. Naast de oorspronkelijke gegevenscategorieën van het eerstegeneratiesysteem kan in SIS II ook worden gewerkt met vingerafdrukken, foto's, en kopieën van het Europees aanhoudingsbevel; tevens kunnen de belangen van personen van wie de identiteit wordt misbruikt, worden beschermd en kunnen links worden gelegd tussen verschillende signaleringen. Zo kan SIS II de signalering betreffende een persoon die wordt gezocht wegens

---

10 Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108 van de Raad van Europa van 28.1.1981 (verdrag nr. 108 van de Raad van Europa); Aanbeveling nr. R(87) 15 van het Comité van Ministers tot regeling van het gebruik van persoonsgegevens op politieel gebied, Raad van Europa, 17.9.1987 (politieaanbeveling).

11 Sirene staat voor Supplemtary Information Request at National Entry.

12 Raadsdocument 5441/08 van 30.1.2008; Raadsdocument 6162/10 van 5.2.2010.

13 Verordening (EG) nr. 1986/2006, PB L 381 van 28.12.2006, blz. 1; Verordening (EG) nr. 1987/2006, PB L 381 van 28.12.2006, blz. 4; Besluit 2007/533/JBZ, PB L 205 van 7.8.2007, blz. 63.

ontvoering, koppelen aan de signalering betreffende de ontvoerde persoon en die betreffende het voertuig dat bij dit strafbare feit werd gebruikt. De toegangsrechten en de regels inzake de bewaring van de gegevens zijn hetzelfde als voor het systeem van de eerste generatie. Persoonsgegevens mogen alleen worden gebruikt voor het doel van de signalering waarvoor ze werden verstrekt. Persoonsgegevens in SIS II moeten worden verwerkt overeenkomstig de specifieke bepalingen van de basisbesluiten betreffende dit systeem (Verordening (EG) nr. 1987/2006 en Besluit 2007/533/JBZ van de Raad) waarin de beginselen van Richtlijn 95/46/EG worden toegelicht, en overeenkomstig Verordening nr. 45/2001, verdrag nr. 108 van de Raad van Europa en de politieaanbeveling[14]. SIS II zal gebruikmaken van s-Testa, het beveiligde communicatienetwerk van de Commissie[15]. Als het systeem eenmaal operationeel is, zal het in alle lidstaten, Zwitserland, Liechtenstein, Noorwegen en IJsland worden gebruikt[16]. De Commissie is verplicht elk half jaar bij het Europees Parlement en de Raad een voortgangsverslag in te dienen over de ontwikkeling van SIS II en de migratie van het systeem van de eerste generatie naar het systeem van de tweede generatie[17].

De ontwikkeling van **EURODAC** kan worden teruggevoerd op de afschaffing van de binnengrenzen, die duidelijke regels voor de behandeling van asielverzoeken noodzakelijk maakte. Eurodac is een centraal geautomatiseerd vingerafdrukidentificatiesysteem dat de vingerafdrukgegevens van bepaalde onderdanen van derde landen bevat. Eurodac is in januari 2003 in gebruik genomen en moet de lidstaten helpen vast te stellen welk land volgens de Dublin-verordening verantwoordelijk is voor de behandeling van een asielverzoek[18]. Van personen van 14 jaar en ouder die asiel aanvragen in een lidstaat, worden automatisch de vingerafdrukken genomen, evenals van onderdanen van derde landen die worden aangehouden omdat zij illegaal een buitengrens hebben overschreden. Door deze vingerafdrukken te vergelijken met de gegevens in Eurodac kunnen de nationale autoriteiten proberen vast te stellen of de betrokkene wellicht al eerder een asielverzoek heeft ingediend, of dat hij voor het eerst in de Europese Unie aankomt. De autoriteiten mogen ook de vingerafdrukken van onderdanen van derde landen die illegaal op hun grondgebied verblijven, vergelijken met de gegevens in Eurodac. De lidstaten moeten aangeven welke autoriteiten toegang hebben tot deze gegevensbank; meestal zijn dat de asiel- en migratieautoriteiten, de grenswacht en de politie. De lidstaten uploaden de gegevens via hun nationale toegangspunt in de centrale gegevensbank. Persoonsgegevens in Eurodac mogen alleen worden gebruikt om de toepassing van de Dublinverordening goed mogelijk te maken; op elk ander gebruik staan

---

14 Verordening (EG) nr. 1987/2006, PB L 381 van 28.12.2006, blz. 4; Besluit 2007/533/JBZ, PB L 205 van 7.8.2007, blz. 63; Richtlijn 95/46/EG, PB L 281 van 23.11.1995, blz. 31; Verordening (EG) nr. 45/2001, PB L 8 van 12.12001, blz. 1; Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108 van de Raad van Europa van 28.1.1981 (verdrag nr. 108 van de Raad van Europa); Aanbeveling nr. R(87) 15 van het Comité van Ministers tot regeling van het gebruik van persoonsgegevens op politieel gebied, Raad van Europa, 17.9.1987 (politieaanbeveling).

15 S-Testa (Secure trans-European services for Telematics between administrations), is een door de Commissie gefinancierd datacommunicatienetwerk voor de veilige en versleutelde uitwisseling van gegevens tussen nationale overheidsdiensten en de EU-instellingen en -organen.

16 Het Verenigd Koninkrijk en Ierland nemen ook deel aan SIS II, behalve als het gaat om signaleringen van onderdanen van derde landen met een inreisverbod.

17 Verordening (EG) nr. 1104/2008 van de Raad, PB L 299 van 8.11.2008, blz. 1; Besluit 2008/839/JBZ van de Raad, PB L 299 van 8.11.2008, blz. 43.

18 Verordening (EG) nr. 343/2003 van de Raad, PB L 50 van 25.2.2003, blz. 1 (Dublinverordening), Verordening (EG) nr. 2725/2000 van de Raad, PB L 316 van 15.12.2000, blz. 1 (Eurodac-verordening). Deze instrumenten vloeien voort uit de Overeenkomst van Dublin van 1990 (PB C 254 van 19.8.1997, blz. 1), die was bedoeld om vast te stellen welke lidstaat een asielverzoek moest behandelen. Het systeem voor het behandelen van asielverzoeken wordt het "Dublinsysteem" genoemd.

sancties. De vingerafdrukken van asielzoekers worden tien jaar bewaard; die van illegale migranten twee jaar. De gegevens van asielzoekers worden verwijderd zodra de betrokkene het burgerschap van een lidstaat verkrijgt; die van illegale migranten zodra zij een verblijfsvergunning of het burgerschap verkrijgen, of wanneer zij het grondgebied van de lidstaten verlaten. Richtlijn 95/46/EG is van toepassing op de verwerking van persoonsgegevens in het kader van dit instrument[19]. Eurodac werkt via het s-Testa-netwerk van de Commissie en wordt gebruikt in alle lidstaten en in Noorwegen, IJsland en Zwitserland. Een overeenkomst betreffende de aansluiting van Liechtenstein is gereed om te worden gesloten. De Commissie moet jaarlijks bij het Europees Parlement en de Raad een verslag indienen over de werking van de centrale eenheid van Eurodac.

In de nasleep van de aanslagen van 11 september 2001 besloten de lidstaten vaart te zetten achter de invoering van een gemeenschappelijk visumbeleid en een netwerk voor de uitwisseling van informatie over visa voor kort verblijf op te zetten[20]. Door de afschaffing van de binnengrenzen is het gemakkelijker geworden om misbruik te maken van de visumregelingen van de lidstaten. Het **Visuminformatiesysteem** (VIS) moet op beide fronten helpen: het is bedoeld als hulpmiddel bij de invoering van een gemeenschappelijk visumbeleid, want het vereenvoudigt de behandeling van visumaanvragen en de controles aan de buitengrenzen, en het helpt tegelijkertijd bedreigingen van de interne veiligheid van de lidstaten voorkomen[21]. Het VIS wordt een gecentraliseerd informatiesysteem met een nationaal deel in elk van de deelnemende lidstaten en een technisch ondersteunende functie in Frankrijk. Het werkt met een biometrisch matchingsysteem dat borg staat voor een betrouwbare vergelijking van vingerafdrukken en het zal worden gebruikt om de identiteit van visumhouders aan de buitengrenzen te controleren. In het systeem worden gegevens over visumaanvragen, foto's, vingerafdrukken, aanverwante besluiten van visumautoriteiten en links tussen aanvragen die met elkaar te maken hebben, opgenomen. Visum-, asiel-, immigratie- en grensbewakingsautoriteiten krijgen toegang tot deze database om de identiteit van visumhouders en de echtheid van visa te controleren. De politie en Europol mogen het VIS raadplegen met het oog op het voorkomen en bestrijden van terrorisme en andere vormen van ernstige criminaliteit[22]. Aanvraagdossiers mogen vijf jaar worden bewaard. Persoonsgegevens in VIS moeten worden verwerkt overeenkomstig de specifieke bepalingen van de basisbesluiten betreffende dit systeem (Verordening (EG) nr. 767/2008 en Besluit 2008/633/JBZ van de Raad), die een aanvulling vormen op de bepalingen van Richtlijn 95/46/EG, Verordening (EG) nr. 45/2001, Kaderbesluit 2008/977/JBZ van de Raad, verdrag nr. 108 van de Raad van Europa, het aanvullend protocol en de politieaanbeveling[23]. Het VIS

---

19 Richtlijn 95/46/EG, PB L 281 van 23.11.1995, blz. 31.

20 Buitengewone Raad Justitie en Binnenlandse zaken van 20.9.2001.

21 Beschikking 2004/512/EG van de Raad, PB L 213 van 15.6.2004, blz. 5; Verordening (EG) nr. 767/2008, PB L 218 van 13.8.2008, blz. 60; Besluit 2008/633/JBZ van de Raad, PB L 218 van 13.8.2008, blz. 129. Zie ook de verklaring betreffende de bestrijding van terrorisme van de Europese Raad van 25.3.2004.

22 Besluit 2008/633/JBZ van de Raad, PB L 218 van 13.8.2008, blz. 129.

23 Verordening (EG) nr. 767/2008, PB L 218 van 13.8.2008, blz. 60; Besluit 2008/633/JBZ van de Raad, PB L 218 van 13.8.2008, blz. 129. Richtlijn 95/46/EG, PB L 281 van 23.11.1995, blz. 31; Verordening (EG) nr. 45/2001, PB L 8 van 12.12001, blz. 1; Kaderbesluit 2008/977/JBZ van de Raad, PB L 350 van 30.12.2008, blz. 60; Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108 van de Raad van Europa van 28.1.1981 (verdrag nr. 108 van de Raad van Europa); Aanvullend protocol bij het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens inzake toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens (ETS nr. 181) van de Raad van Europa van 8.11.2001 (aanvullend protocol 181); Aanbeveling nr. R(87) 15 van het Comité van Ministers tot

zal van toepassing zijn in alle lidstaten behalve het Verenigd Koninkrijk en Ierland, alsmede in Zwitserland, Noorwegen en IJsland. Het werkt via het s-Testa-netwerk van de Commissie. De Commissie zal het systeem drie jaar na de ingebruikneming evalueren en daarna elke vier jaar.

Op initiatief van Spanje heeft de Raad in 2004 een richtlijn vastgesteld die de doorgifte van **op voorhand af te geven passagiersgegevens (Advance Passenger Information, API)** aan grensbewakingsautoriteiten door luchtvaartmaatschappijen regelt[24]. Dit instrument is bedoeld om de grensbewaking te verbeteren en illegale migratie te bestrijden. Luchtvaartmaatschappijen moeten de grensbewakingsautoriteiten desgevraagd de naam, de geboortedatum, de nationaliteit, het instappunt en de grensdoorlaatpost van binnenkomst van passagiers die vanuit derde landen naar de EU reizen, doorgeven. Dergelijke gegevens worden doorgaans verkregen van het machineleesbare gedeelte van het paspoort van de passagiers en doorgegeven aan de autoriteiten na de check-in. De autoriteiten en de luchtvaartmaatschappijen mogen de API-gegevens tot 24 uur na aankomst van de vlucht bewaren. Het API-systeem werkt op gedecentraliseerde wijze op basis van informatie-uitwisseling tussen particuliere maatschappijen en overheidsdiensten. Dit instrument laat de uitwisseling van API tussen de lidstaten niet toe. Andere rechtshandhavingsautoriteiten dan de grenswacht mogen echter ook om toegang tot deze informatie vragen voor rechtshandhavingsdoeleinden. Persoonsgegevens mogen door overheidsdiensten alleen worden gebruikt om grenscontroles te verrichten en om illegale migratie te bestrijden, en moeten worden verwerkt overeenkomstig Richtlijn 95/46/EG[25]. Dit instrument is weliswaar van kracht in de gehele EU, maar wordt slechts door een beperkt aantal lidstaten gebruikt. De Commissie zal de richtlijn in 2011 evalueren.

Een belangrijk deel van het 1992-programma van de Commissie waarmee de interne markt tot stand werd gebracht, had betrekking op de afschaffing van alle controles en formaliteiten ten aanzien van het goederenverkeer in de Gemeenschap[26]. Door de afschaffing van dergelijke procedures aan de binnengrenzen nam het risico op fraude toe, waardoor de lidstaten een mechanisme van wederzijdse administratieve bijstand in het leven moesten roepen om elkaar te helpen bij het voorkomen, onderzoeken en vervolgen van transacties die niet strookten met de communautaire douane- en landbouwwetgeving, en tevens een douanesamenwerking tot stand moesten brengen om het opsporen en vervolgen van inbreuken op de nationale douanevoorschriften mogelijk te maken, met name door middel van een betere grensoverschrijdende informatie-uitwisseling. Zonder afbreuk te doen aan de bevoegdheden van de EU in de douane-unie moet de **Napels II-overeenkomst** inzake wederzijdse bijstand en samenwerking tussen de douaneadministraties de nationale douanediensten in staat stellen inbreuken op de nationale douanevoorschriften te voorkomen en op te sporen en hen helpen inbreuken op de communautaire en de nationale douanevoorschriften te vervolgen en te bestraffen[27]. In het kader van dit instrument kunnen de centrale coördinatie-eenheden schriftelijk om bijstand verzoeken van hun tegenhangers in de andere lidstaten in

---

regeling van het gebruik van persoonsgegevens op politieel gebied, Raad van Europa, 17.9.1987 (politieaanbeveling).

24 Richtlijn 2004/82/EG van de Raad, PB L 261 van 6.8.2004, blz. 24.

25 Richtlijn 95/46/EG, PB L 281 van 23.11.1995, blz. 31.

26 Verordening (EEG) nr. 2913/92 van de Raad, PB L 302 van 19.10.1992.

27 Verordening (EG) nr. 515/97 van de Raad van 13 maart 1997 betreffende de wederzijdse bijstand tussen de administratieve autoriteiten van de lidstaten en de samenwerking tussen deze autoriteiten en de Commissie met het oog op de juiste toepassing van de douane- en landbouwvoorschriften, PB L 82 van 22.3.1997, blz.1, gewijzigd bij Verordening (EG) nr. 766/2002, PB L 218 van 13.8.2008, blz. 48.

strafrechtelijke onderzoeken in verband met inbreuken op de nationale en de communautaire douanevoorschriften[28]. Deze eenheden mogen alleen persoonsgegevens verwerken in het kader van de Napels II-overeenkomst. Zij mogen deze gegevens doorgeven aan nationale douaneautoriteiten, onderzoeksautoriteiten en gerechtelijke instanties, en, met voorafgaande toestemming van de lidstaat die de gegevens verstrekt, aan andere autoriteiten. De gegevens mogen niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor ze werden verstrekt. Persoonsgegevens moeten in de ontvangende lidstaat ten minste hetzelfde beschermingsniveau genieten als in de verstrekkende lidstaat en zij moeten worden verwerkt overeenkomstig Richtlijn 95/46/EG en verdrag nr. 108 van de Raad van Europa[29]. Alle lidstaten hebben de Napels II-overeenkomst geratificeerd. Zij kunnen wijzigingen van de overeenkomst voorstellen, waarna de gewijzigde tekst moet worden goedgekeurd door de Raad van ministers en geratificeerd door de lidstaten.

Ter aanvulling van de Napels II-overeenkomst wordt bij de DIS-overeenkomst het **Douane-informatiesysteem** (DIS) ingevoerd, dat moet bijdragen tot het voorkomen, onderzoeken en vervolgen van ernstige overtredingen van de nationale wetten door een betere samenwerking tussen de douaneadministraties van de lidstaten, op basis van een snelle verspreiding van informatie[30]. Het DIS, dat wordt beheerd door de Commissie, is een gecentraliseerd informatiesysteem dat toegankelijk is via terminals in elke lidstaat, en bij de Commissie, Europol en Eurojust. Het systeem bevat persoonsgegevens met betrekking tot goederen, vervoermiddelen, bedrijven en personen en ingehouden, in beslag genomen of geconfisqueerde goederen en contanten. De persoonsgegevens omvatten namen en aliassen, geboortedatum en –plaats, nationaliteit, geslacht, fysieke kenmerken, identiteitsdocumenten, adres, eerder voorgekomen gewelddadigheid, de reden voor het opnemen van de gegevens in het DIS, de voorgestelde actie en de registratiekenmerken van vervoermiddelen. Als het gaat om ingehouden, in beslag genomen of geconfisqueerde goederen en contanten mogen alleen biografische gegevens en adressen in het DIS worden ingevoerd. Deze gegevens mogen uitsluitend worden gebruikt voor melding van waarneming of voor het verrichten van onopvallende of gerichte controles en strategische of operationele analyses met betrekking tot personen die worden verdacht van het overtreden van de nationale douanevoorschriften. De nationale douane-, belasting-, landbouw-, volksgezondheids- en politieautoriteiten, Europol en Eurojust hebben toegang tot de DIS-gegevens[31]. De verwerking van persoonsgegevens moet gebeuren overeenkomstig de regels van de DIS-overeenkomst en de bepalingen van Richtlijn 95/46/EG, Verordening (EG) nr. 45/2001, verdrag nr. 108 van de Raad van Europa en de politieaanbeveling[32]. Persoonsgegevens mogen vanuit het DIS alleen naar andere

---

28 Overeenkomst opgesteld op grond van artikel K.3 van het Verdrag betreffende de Europese Unie inzake wederzijdse bijstand en samenwerking tussen de douaneadministraties, PB C 24 van 23.1.1998 (Napels II-overeenkomst).

29 Richtlijn 95/46/EG, PB L 281 van 23.11.1995, blz. 31; Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108 van de Raad van Europa van 28.1.1981 (verdrag nr. 108 van de Raad van Europa).

30 Overeenkomst opgesteld op grond van artikel K.3 van het Verdrag betreffende de Europese Unie inzake het gebruik van informatica op douanegebied, PB C 316 van 27.11.1995, blz. 34, gewijzigd bij Besluit 2009/917/JBZ van de Raad, PB L 323 van 10.12.2009, blz. 20.

31 Vanaf mei 2011 hebben Europol en Eurojust inzage in het DIS op basis van Besluit 2009/917/JBZ van de Raad (PB L 323 van 10.12.2009, blz. 20).

32 Overeenkomst opgesteld op grond van artikel K.3 van het Verdrag betreffende de Europese Unie inzake het gebruik van informatica op douanegebied, PB C 316 van 27.11.1995, blz. 34, gewijzigd bij Besluit 2009/917/JBZ van de Raad, PB L 323 van 10.12.2009, blz. 20; Richtlijn 95/46/EG, PB L 281 van 23.11.1995, blz. 31; Verordening (EG) nr. 45/2001, PB L 8 van 12.12001, blz. 1; Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens

gegevensverwerkingssystemen worden gekopieerd ten behoeve van risicobeheer of operationele analyses, die alleen toegankelijk zijn voor de door de lidstaten aangewezen analisten. Uit het DIS gekopieerde persoonsgegevens mogen slechts bewaard blijven zolang dat nodig is om het doel waarvoor ze werden gekopieerd, te verwezenlijken, en in geen geval langer dan tien jaar. Ook het **referentiebestand van onderzoeksdossiers op douanegebied** (FIDE) maakt deel uit van het DIS en is een hulpmiddel bij het voorkomen, onderzoeken en vervolgen van ernstige overtredingen van de nationale wetten[33]. In het FIDE kunnen de nationale autoriteiten die bevoegd zijn voor douaneonderzoeken bij het begin van een onderzoek nagaan welke andere autoriteiten onderzoek verrichten of hebben verricht naar bepaalde personen of bedrijven. Deze autoriteiten mogen in het FIDE gegevens uit hun onderzoeksdossier invoeren, zoals de biografische gegevens van personen naar wie een onderzoek loopt en de firmanaam, de handelsnaam, het btw-identificatienummer en het adres van bedrijven waarnaar een onderzoek is ingesteld. Gegevens uit onderzoeksdossiers waarin geen douanefraude is vastgesteld, mogen maximaal drie jaar worden bewaard, gegevens uit onderzoeksdossiers waarin wel douanefraude is vastgesteld, maximaal zes jaar, en gegevens uit dossiers waarin een veroordeling is uitgesproken of een boete is opgelegd, maximaal tien jaar. Het DIS en het FIDE maken gebruik van het gemeenschappelijk communicatienetwerk, de gemeenschappelijke systeeminterface of de beveiligde internettoegang van de Commissie. Het DIS is in gebruik in alle lidstaten. De Commissie brengt elk jaar in samenwerking met de lidstaten verslag uit aan het Europees Parlement en de Raad over de werking van het DIS.

EU-instrumenten ter voorkoming en bestrijding van terrorisme en andere vormen van ernstige grensoverschrijdende criminaliteit

De terreuraanslagen in Madrid in maart 2004 hebben geleid tot verschillende nieuwe initiatieven op EU-niveau. Op verzoek van de Europese Raad heeft de Commissie in 2005 een voorstel ingediend voor een instrument dat de uitwisseling van informatie op basis van het beschikbaarheidsbeginsel moet regelen[34]. In plaats van dit voorstel heeft de Raad in 2006 een **Zweeds initiatief** goedgekeurd dat de uitwisseling regelt van bestaande informatie en inlichtingen die noodzakelijk kunnen zijn voor een strafrechtelijk onderzoek of een criminele-inlichtingenoperatie[35]. Dit instrument is gebaseerd op het beleidsbeginsel "gelijkwaardige toegang", dat inhoudt dat de voorwaarden voor grensoverschrijdende gegevensuitwisseling niet strikter mogen zijn dan die welke gelden voor de binnenlandse toegang. Het Zweedse initiatief werkt decentraal en biedt politie, douane en andere autoriteiten die bevoegd zijn strafbare feiten te onderzoeken (met uitzondering van de inlichtingendiensten, die doorgaans werken met inlichtingen betreffende de nationale of de staatsveiligheid) de mogelijkheid informatie en criminele inlichtingen uit te wisselen met hun collega's binnen de EU. De lidstaten moeten nationale contactpunten aanwijzen die dringende verzoeken om informatie moeten behandelen. Dit kaderbesluit stelt duidelijke termijnen voor de uitwisseling van

---

(ETS nr. 108 van de Raad van Europa van 28.1.1981 (verdrag nr. 108 van de Raad van Europa); Aanbeveling nr. R(87) 15 van het Comité van Ministers tot regeling van het gebruik van persoonsgegevens op politieel gebied, Raad van Europa, 17.9.1987 (politieaanbeveling).

33 FIDE staat voor *Fichier d'Identification des Dossiers d'Enquête douanières*; dit referentiebestand is gebaseerd op Verordening (EG) nr. 766/2008 en het Protocol vastgesteld overeenkomstig artikel 34 van het Verdrag betreffende de Europese Unie tot wijziging, wat betreft de vorming van een referentiebestand van onderzoeksdossiers op douanegebied, van de Overeenkomst inzake het gebruik van informatica op douanegebied, PB C 139 van 13.6.2003, blz. 1.

34 COM(2005) 490 van 12.10.2005; Conclusies van het voorzitterschap – Het Haags programma, 4/5.11.2004. Zie ook de verklaring betreffende de bestrijding van terrorisme van de Europese Raad van 25.3.2004.

35 Kaderbesluit 2006/960/JBZ van de Raad, PB L 386 van 29.12.2006, blz. 89.

informatie en verplicht de lidstaten een formulier in te vullen als zij gegevens willen opvragen. De lidstaten moeten in spoedeisende gevallen binnen acht uur antwoorden op verzoeken om informatie of inlichtingen, in niet-spoedeisende gevallen binnen een week en in alle andere gevallen binnen twee weken. Het gebruik van de informatie en inlichtingen die via dit instrument zijn verkregen, is onderworpen aan de nationale gegevensbeschermingsvoorschriften; de lidstaten mogen daarbij geen onderscheid maken tussen gegevens waarover zij zelf beschikken en gegevens die afkomstig zijn van andere lidstaten. De verstrekkende lidstaat mag echter wel voorwaarden verbinden aan het gebruik van de informatie of inlichtingen in andere lidstaten. Persoonsgegevens moeten worden verwerkt overeenkomstig de nationale gegevensbeschermingswetgeving en verdrag nr. 108 van de Raad van Europa, aanvullend protocol nr. 181 en de politieaanbeveling[36]. 12 van de 31 ondertekenende partijen (EU-lidstaten, Noorwegen, IJsland, Zwitserland en Liechtenstein) hebben nationale wetgeving vastgesteld om het kaderbesluit om te zetten; vijf staten vullen regelmatig het formulier in dat moet worden gebruikt bij een verzoek om informatie, maar slechts twee staten gebruiken het frequent om informatie uit te wisselen[37]. De Commissie zal haar evaluatieverslag voor eind 2010 indienen bij de Raad.

Het **Prümbesluit** bouwt voort op het verdrag dat in 2005 door Duitsland, Frankrijk, Spanje, de Benelux en Oostenrijk werd gesloten om de grensoverschrijdende samenwerking bij de bestrijding van terrorisme, grensoverschrijdende criminaliteit en illegale migratie te intensiveren. Toen verschillende lidstaten kenbaar maakten dat zij tot dit verdrag wilden toetreden, stelde Duitsland tijdens zijn voorzitterschap van de Raad in 2007 voor om het verdrag om te vormen tot een EU-instrument. Het Prümbesluit van 2008, dat vanaf augustus 2011 volledig moet worden toegepast, stelt de regels vast voor de grensoverschrijdende uitwisseling van DNA-profielen, vingerafdrukken, gegevens uit kentekenregisters en gegevens over personen die worden verdacht van het beramen van terroristische aanslagen[38]. Het besluit moet de preventie van strafbare feiten, met name terrorisme en grensoverschrijdende criminaliteit, verbeteren en de openbare orde bij grootschalige evenementen helpen handhaven. Dit gebeurt aan de hand van een decentraal systeem waarbij de DNA-, vingerafdruk- en kentekendatabases van de deelnemende landen via nationale contactpunten met elkaar zijn verbonden. Via het s-Testa-netwerk van de Commissie behandelen de contactpunten inkomende en uitgaande verzoeken om grensoverschrijdende vergelijking van DNA-profielen, vingerafdrukken en gegevens uit kentekenregisters. Hun bevoegdheden om deze gegevens door te geven aan de eindgebruikers, worden geregeld bij nationaal recht. Vanaf augustus 2011 zal de gegevensvergelijking volledig geautomatiseerd verlopen. De lidstaten moeten echter een grondige evaluatie ondergaan (waarbij in het bijzonder wordt nagegaan of zij voldoen aan de technische vereisten en de gegevensbeschermingsvoorschriften) voordat zij met de automatische gegevensuitwisseling

---

[36] Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108 van de Raad van Europa van 28.1.1981 (verdrag nr. 108 van de Raad van Europa); Aanvullend protocol bij het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens inzake toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens (ETS nr. 181) van de Raad van Europa van 8.11.2001 (aanvullend protocol 181); Aanbeveling nr. R(87) 15 van het Comité van Ministers tot regeling van het gebruik van persoonsgegevens op politieel gebied, Raad van Europa, 17.9.1987 (politieaanbeveling).

[37] Deze gegevens zijn gebaseerd op de antwoorden op een vragenlijst, waarvan de resultaten door het Spaanse voorzitterschap zijn gepresenteerd tijdens een bijeenkomst van de ad-hocwerkgroep van de Raad voor informatie-uitwisseling op 22 juni 2010.

[38] Besluit 2008/615/JBZ van de Raad, PB L 210 van 6.8.2008, blz. 1; Besluit 2008/616/JBZ van de Raad, PB L 210 van 6.8.2008, blz. 12.

mogen beginnen. In het kader van dit instrument mogen geen persoonsgegevens worden uitgewisseld voordat de lidstaten een gegevensbeschermingsniveau garanderen dat op zijn minst gelijk is aan het niveau dat beantwoordt aan verdrag nr. 108 van de Raad van Europa, aanvullend protocol 181 en de politieaanbeveling[39]. De Raad besluit met eenparigheid van stemmen of aan deze voorwaarde is voldaan. Persoonsgegevens mogen uitsluitend worden gebruikt voor het doel waarvoor ze worden verstrekt, tenzij de verstrekkende lidstaat instemt met het gebruik voor andere doeleinden. Personen kunnen zich ook tot de op grond van Richtlijn 95/46/EG aangewezen nationale gegevensbeschermingsfunctionarissen richten om hun rechten inzake de verwerking van persoonsgegevens in het kader van dit instrument af te dwingen. De vergelijking van DNA-profielen en vingerafdrukken gebeurt op basis van een (anoniem) hit/no hit-systeem, waarbij autoriteiten alleen aanvullende persoonsgegevens mogen opvragen als de bevraging een hit heeft opgeleverd. Deze verzoeken om aanvullende informatie worden meestal op basis van het Zweedse initiatief ingediend. Het Prümbesluit wordt uitgevoerd in de 27 lidstaten; Noorwegen en IJsland sluiten zich er binnenkort bij aan[40]. De Commissie zal haar evaluatieverslag in 2012 indienen bij de Raad.

Naar aanleiding van de bomaanslagen in Londen in 2005 hebben het Verenigd Koninkrijk, Ierland, Zweden en Frankrijk een EU-instrument voorgesteld ter harmonisering van de nationale regels voor gegevensbewaring. De **richtlijn gegevensbewaring** uit 2006 verplicht aanbieders van telefoon- en internetdiensten om verkeers- en locatiegegevens over elektronische communicatie, alsmede gegevens over abonnees (zoals telefoonnummer, IP-adres en identificatiecode voor mobiele apparatuur) te bewaren zodat ze kunnen worden gebruikt voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit[41]. De richtlijn gegevensbewaring regelt niet de toegang tot of het gebruik van gegevens die door nationale autoriteiten worden bewaard. De inhoud van elektronische communicatie valt uitdrukkelijk buiten de werkingssfeer van de richtlijn. Aftappen is dus niet mogelijk in het kader van dit instrument. Deze richtlijn laat de definitie van "ernstige criminaliteit" over aan de lidstaten. De lidstaten bepalen ook welke nationale autoriteiten in welke gevallen toegang hebben tot de gegevens, en welke procedures en voorwaarden daarvoor gelden. De bewaartermijnen variëren van 6 tot 24 maanden. Richtlijn 95/46/EG en Richtlijn 2002/58/EG zijn van toepassing op de bescherming van persoonsgegevens in het kader van dit instrument[42]. Zes lidstaten hebben de richtlijn nog niet volledig omgezet en het constitutionele hof van Duitsland en dat van Roemenië hebben de nationale omzettingsmaatregelen ongrondwettig verklaard. Het Duitse constitutionele hof heeft de nationale wettelijke regels voor de toegang tot en het gebruik van de gegevens ongrondwettig bevonden[43]. Het Roemeense constitutionele hof heeft geoordeeld dat gegevensbewaring per se in strijd is met

---

39 Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108 van de Raad van Europa van 28.1.1981 (verdrag nr. 108 van de Raad van Europa); Aanvullend protocol bij het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens inzake toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens (ETS nr. 181) van de Raad van Europa van 8.11.2001 (aanvullend protocol 181); Aanbeveling nr. R(87) 15 van het Comité van Ministers tot regeling van het gebruik van persoonsgegevens op politieel gebied, Raad van Europa, 17.9.1987 (politieaanbeveling).

40 Tot nu toe hebben tien lidstaten toestemming gekregen voor de automatische uitwisseling van DNA-profielen, vijf voor de automatische uitwisseling van vingerafdrukken en zeven voor die van gegevens uit kentekenregisters. Duitsland, Oostenrijk, Spanje en Nederland hebben de Commissie gedeeltelijke statistieken verstrekt over het gebruik van dit instrument.

41 Richtlijn 2006/24/EG, PB L 105 van 13.4.2006, blz. 54.

42 Richtlijn 95/46/EG, PB L 281 van 23.11.1995, blz. 31; Richtlijn 2002/58/EG, PB L 201 van 31.7.2002, blz. 37 (richtlijn e-privacy).

43 Arrest van het Duitse constitutionele hof, Bundesverfassunggericht 1 BvR 256/08 van 11.3.2008.

artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (Europees mensenrechtenverdrag), en dus ongrondwettig is[44]. De Commissie werkt momenteel aan een evaluatie van dit instrument en zal eind 2010 haar evaluatieverslag indienen bij het Europees Parlement en de Raad.

De oprichting van het **Europees strafregisterinformatiesysteem** (Ecris), waaraan nog wordt gewerkt, vloeit voort uit een Belgisch initiatief uit 2004 dat was bedoeld om veroordeelde zedendelinquenten het recht te ontnemen in andere lidstaten met kinderen te werken. In het verleden maakten de lidstaten gebruik van het Verdrag aangaande de wederzijdse rechtshulp in strafzaken van de Raad van Europa om informatie uit te wisselen over veroordelingen van hun onderdanen, maar dit systeem bleek niet efficiënt te werken[45]. De Raad zette een eerste stap op weg naar verbetering met de goedkeuring van Besluit 2005/876/JBZ van de Raad, dat de lidstaten verplichtte een centrale autoriteit aan te wijzen die regelmatig gegevens over veroordelingen van niet-onderdanen moest verstrekken aan de lidstaat of lidstaten waarvan de betrokkene de nationaliteit had[46]. Dit instrument bood de lidstaten ook voor het eerst de mogelijkheid om, volgens de voorwaarden van het nationale recht, gegevens te verkrijgen over eerdere veroordelingen van hun onderdanen in andere lidstaten. Deze gegevens konden zij opvragen via een standaardformulier in plaats van via procedures voor wederzijdse rechtshulp. In 2006 en 2007 heeft de Commissie een wetgevingspakket gepresenteerd bestaande uit drie instrumenten: Kaderbesluit 2008/675/JBZ van de Raad, dat de lidstaten verplicht bij een nieuwe strafrechtelijke procedure rekening te houden met eerdere veroordelingen in andere lidstaten, Kaderbesluit 2009/315/JBZ van de Raad betreffende de organisatie en de inhoud van uitwisseling van gegevens uit het strafregister, en Besluit 2009/316/JBZ van de Raad tot oprichting van Ecris als het technische instrument voor de uitwisseling van gegevens uit het strafregister[47]. Kaderbesluit 2009/315/JBZ van de Raad en Besluit 2009/316/JBZ van de Raad, die uiterlijk in april 2012 volledig moeten worden toegepast, hebben ten doel voor te schrijven hoe de veroordelende lidstaat gegevens over een nieuwe veroordeling moet doorgeven aan de lidstaat of lidstaten waarvan de veroordeelde de nationaliteit bezit, vast te stellen welke opslagverplichtingen moet worden nageleefd en een kader te schetsen voor een elektronisch gegevensuitwisselingssysteem. Ecris wordt een gedecentraliseerd informatiesysteem dat de strafregisters van de lidstaten met elkaar verbindt via het s-Testa-netwerk van de Commissie. Centrale autoriteiten zullen gegevens uitwisselen over nieuwe veroordelingen en veroordelingen uit het verleden. De gegevens worden versleuteld en gestructureerd volgens een vooraf bepaald formaat en omvatten biografische gegevens, de veroordeling, de straf en het aan de veroordeling ten grondslag liggende strafbare feit en aanvullende informatie (zoals vingerafdrukken, indien beschikbaar). Vanaf april 2012 moeten voor lopende strafrechtelijke procedures uittreksels van strafregisters worden verstrekt aan de gerechtelijke of de bevoegde administratieve autoriteiten, zoals instanties die bevoegd zijn om personen door te lichten in verband met een gevoelige positie of vuurwapenbezit. Persoonsgegevens die worden verstrekt voor strafrechtelijke procedures mogen alleen voor dat doel worden gebruikt; voor het gebruik voor andere doeleinden is de toestemming van de lidstaat die de gegevens heeft verstrekt, vereist. De verwerking van persoonsgegevens moet gebeuren overeenkomstig de desbetreffende bepalingen van

---

44 Beslissing nr. 1258 van het Roemeense constitutionele hof van 8.10.2009.

45 Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken (ETS nr. 30), Raad van Europa, van 20.4.1959. Zie ook COM(2005) 10 van 25.1.2005.

46 Besluit 2005/876/JBZ van de Raad, PB L 322 van 9.12.2005, blz. 33.

47 Kaderbesluit 2008/675/JBZ van de Raad, PB L 220 van 15.8.2008, blz. 32; Kaderbesluit 2009/315/JBZ van de Raad, PB L 93 van 7.4.2009, blz. 23; Besluit 2009/316/JBZ van de Raad, PB L 93 van 7.4.2009, blz. 33. Zie ook COM(2005) 10 van 25.1.2005.

Kaderbesluit 2009/315/JBZ van de Raad, waarin de regels van Besluit 2005/876/JBZ zijn verwerkt, en overeenkomstig Kaderbesluit 2008/977/JBZ van de Raad en verdrag nr. 108 van de Raad van Europa[48]. Als de EU-instellingen persoonsgegevens verwerken via Ecris, bijvoorbeeld om gegevens te beveiligen, is Verordening (EG) 45/2001 van toepassing[49]. Dit wetgevingspakket bevat geen regels voor de bewaring van gegevens, omdat de opslag van gegevens over strafrechtelijke veroordelingen wordt geregeld bij nationaal recht. Vijftien lidstaten nemen momenteel deel aan een proefproject; negen daarvan zijn begonnen met de elektronische uitwisseling van gegevens uit het strafregister. De Commissie moet twee evaluatieverslagen aan het Europees Parlement en de Raad voorleggen over de tenuitvoerlegging van dit pakket: Kaderbesluit 2008/675/JBZ wordt in 2011 geëvalueerd en Kaderbesluit 2009/315/JBZ in 2015. Vanaf 2016 moet de Commissie ook regelmatig verslagen opstellen over de werking van Ecris.

Op initiatief van Finland heeft de Raad in 2000 zijn goedkeuring gehecht aan een instrument dat de uitwisseling van gegevens tussen de **financiële inlichtingeneenheden** van de lidstaten (FIE's) ten behoeve van de bestrijding van het witwassen van geld en, later, van de financiering van terroristische activiteiten regelt[50]. FIE's zijn doorgaans eenheden binnen rechtshandhavingsinstanties, justitiële autoriteiten of administratieve organen die aan financiële autoriteiten rapporteren. Zij moeten de verlangde beschikbare financiële informatie en wetshandhavingsgegevens uitwisselen met hun tegenhangers in de andere lidstaten, waaronder gegevens over financiële transacties, behalve wanneer dit niet in verhouding zou staan tot de belangen van een natuurlijke of rechtspersoon. Gegevens die worden verstrekt met het oog op het analyseren of onderzoeken van witwaspraktijken of de financiering van terroristische activiteiten mogen ook worden gebruikt voor strafrechtelijke onderzoeken of vervolging, tenzij de lidstaat die de gegevens verstrekt dit verbiedt. De verwerking van persoonsgegevens moet gebeuren overeenkomstig de bepalingen van Kaderbesluit 2008/977/JBZ van de Raad, verdrag nr. 108 van de Raad van Europa en de politieaanbeveling[51]. In 2002 hebben verschillende lidstaten fiu.net opgericht, een gedecentraliseerd netwerk voor de uitwisseling van gegevens tussen FIE's dat gebruikmaakt van het s-Testa-netwerk van de Commissie[52]. Hierbij zijn twintig FIE's aangesloten. Er wordt nog gesproken over de mogelijkheid om voor fiu.net gebruik te maken van Siena[53], de beveiligde toepassing van Europol. Na een toetsing van de naleving van dit instrument door de lidstaten heeft de Raad FIE's in de derde anti-witwasrichtlijn de bevoegdheid gegeven om meldingen van verdachte transacties die verband houden met witwassen of met de financiering van terrorisme te ontvangen, analyseren en verspreiden[54]. Als onderdeel van haar

---

48 Kaderbesluit 2009/315/JBZ van de Raad, PB L 93 van 7.4.2009, blz. 23; Besluit 2005/876/JBZ van de Raad, PB L 322 van 9.12.2005, blz. 33; Kaderbesluit 2008/977/JBZ van de Raad, PB L 350 van 30.12.2008, blz. 60; Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108 van de Raad van Europa van 28.1.1981 (verdrag nr. 108 van de Raad van Europa).

49 Verordening (EG) nr. 45/2001, PB L 8 van 12.12001, blz. 1.

50 Besluit 2000/642/JBZ van de Raad, PB L 271 van 24.10.2000, blz. 4.

51 Kaderbesluit 2008/977/JBZ van de Raad, PB L 350 van 30.12.2008, blz. 60; Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108 van de Raad van Europa van 28.1.1981 (Verdrag nr. 108 van de Raad van Europa); Aanbeveling nr. R(87) 15 van het Comité van Ministers tot regeling van het gebruik van persoonsgegevens op politieel gebied, Raad van Europa, 17.9.1987 (Politieaanbeveling).

52 http://www.fiu.net/

53 Siena staat voor Secure Information Exchange Network Application.

54 Richtlijn 2005/60/EG, PB L 309 van 25.11.2005, blz. 15 (derde anti-witwasrichtlijn).

Actieplan voor financiële diensten heeft de Commissie de uitvoering van de derde anti-witwasrichtijn sinds 2009 geëvalueerd[55].

Op initiatief van Oostenrijk, België en Finland heeft de Raad in 2007 een instrument vastgesteld ter verbetering van de samenwerking tussen de nationale **bureaus voor de ontneming van vermogensbestanddelen** bij het opsporen en identificeren van opbrengsten van misdrijven[56]. Net als FIE's werken deze bureaus samen op gedecentraliseerde wijze, zij het zonder een onlineplatform. Zij moeten bij het uitwisselen van informatie te werk gaan volgens het Zweedse initiatief, waarbij zo nauwkeurig mogelijke aanwijzingen moeten worden gegeven omtrent de beoogde vermogensbestanddelen (zoals bankrekeningen, vastgoed en voertuigen) en gegevens moeten worden verstrekt over de gezochte natuurlijke of rechtspersonen (zoals naam, adres, geboortedatum en aandeelhouders- en bedrijfsgegevens). Het gebruik van de informatie die via dit instrument is verkregen, is onderworpen aan de nationale gegevensbeschermingsvoorschriften; de lidstaten mogen daarbij geen onderscheid maken tussen gegevens waarover zij zelf beschikken en gegevens die afkomstig zijn van andere lidstaten. Persoonsgegevens moeten worden verwerkt overeenkomstig de bepalingen van verdrag nr. 108 van de Raad van Europa, aanvullend protocol nr. 181 en de politieaanbeveling[57]. Op dit moment hebben ruim twintig lidstaten bureaus voor de ontneming van vermogensbestanddelen opgericht. Gezien de gevoelige aard van de gegevens die worden uitgewisseld, zijn er besprekingen gaande over het gebruik van Siena, de beveiligde toepassing van Europol, voor de uitwisseling van gegevens tussen de bureaus. In een proefproject dat in mei 2010 van start is gegaan, maken twaalf bureaus gebruik van Siena voor het uitwisselen van gegevens over de opsporing van vermogensbestanddelen. De Commissie moet in 2010 een evaluatieverslag indienen bij de Raad.

In 2008 heeft het Franse voorzitterschap de lidstaten verzocht **nationale signaleringsplatformen voor cybercriminaliteit** op te richten en Europol gevraagd hetzelfde te doen op Europees niveau, voor het verzamelen, analyseren en uitwisselen van informatie over inbreuken op internet[58]. Burgers kunnen gevallen van illegale inhoud of gedragingen die zij op internet aantreffen, melden bij hun nationale platform. Het Europees cybercriminaliteitplatform (ECCP), dat wordt beheerd door Europol, moet dienen als informatieknooppunt waar gegevens over cybercriminaliteit die onder de bevoegdheid van Europol valt[59], worden geanalyseerd en met nationale rechtshandhavingsautoriteiten worden uitgewisseld. Bijna alle lidstaten hebben nu een nationaal signaleringsplatform voor

---

55 Zie bijvoorbeeld "Evaluation of the economic impacts of the Financial Services Action Plan – Final report (for European Commission, DG Markt)", CRA International, maart 2009.

56 Besluit 2007/845/JBZ van de Raad, PB L 332 van 18.12.2007, blz. 103.

57 Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108 van de Raad van Europa van 28.1.1981 (verdrag nr. 108 van de Raad van Europa); Aanvullend protocol bij het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens inzake toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens (ETS nr. 181) van de Raad van Europa van 8.11.2001 (aanvullend protocol 181); Aanbeveling nr. R(87) 15 van het Comité van Ministers tot regeling van het gebruik van persoonsgegevens op politieel gebied, Raad van Europa, 17.9.1987 (politieaanbeveling).

58 Conclusies van de Raad over de oprichting van nationale signaleringsplatformen en een Europees signaleringsplatform voor het melden van inbreuken op internet; Raad Justitie en Binnenlandse Zaken van 24.10.2008; conclusies van de Raad over een actieplan ter uitvoering van de gecoördineerde strategie tegen cybercriminaliteit; Raad Algemene Zaken van 26.4.2010. Europol heeft zijn project omgedoopt tot "Europees cybercriminaliteitplatform" (ECCP).

59 Europol heeft als doel het voorkomen en bestrijden van georganiseerde criminaliteit, terrorisme en andere vormen van ernstige criminaliteit waarbij twee of meer lidstaten betrokken zijn. Zie Besluit 2009/371/JBZ van de Raad, PB L 121 van 15.5.2009, blz. 37.

cybercriminaliteit opgericht. Europol werkt aan de technische invoering van het ECCP en kan waarschijnlijk binnenkort zijn Siena-toepassing gebruiken om de gegevensuitwisseling met de nationale platforms te verbeteren. Voor zover bij deze uitwisseling van gegevens door Europol persoonsgegevens worden verwerkt, zijn de specifieke gegevensbeschermingsbepalingen van het Europol-besluit (Besluit 2009/371/JBZ) van toepassing, alsook Verordening (EG) 45/2001, verdrag nr. 108 van de Raad van Europa, aanvullend protocol nr. 181 en de politieaanbeveling[60]. De bepalingen van Kaderbesluit 2008/977/JBZ van de Raad regelen de uitwisseling van persoonsgegevens tussen de lidstaten en Europol[61]. Omdat er geen rechtsinstrument is, is er ook geen formeel evaluatiemechanisme voor de signaleringsplatforms voor cybercriminaliteit. Europol neemt dit belangrijke werk echter al voor zijn rekening en zal in de toekomst verslag uitbrengen over de activiteiten van het ECCP in het jaarverslag, dat ter goedkeuring aan de Raad en ter informatie aan het Europees Parlement wordt voorgelegd.

EU-bureaus en -organen die tot taak hebben de lidstaten bij te staan bij het voorkomen en bestrijden van ernstige grensoverschrijdende criminaliteit

De **Europese politiedienst** (Europol), die in 1995 werd opgericht, begon zijn werkzaamheden in 1999 en werd in januari 2010 een EU-orgaan[62]. Europol moet de lidstaten bijstaan bij het voorkomen en bestrijden van georganiseerde criminaliteit, terrorisme en andere vormen van ernstige criminaliteit waarbij twee of meer lidstaten betrokken zijn. Hoofdtaken zijn het verzamelen, opslaan, verwerken, analyseren en uitwisselen van informatie en inlichtingen, bijstand verlenen bij onderzoeken, en de lidstaten inlichtingen verstrekken en analytische ondersteuning bieden. De belangrijkste schakel tussen Europol en de lidstaten zijn de nationale Europol-eenheden in de lidstaten, die verbindingsofficieren naar Europol afvaardigen. De hoofden van de nationale eenheden komen regelmatig bijeen om Europol bij te staan inzake operationele aangelegenheden; de raad van bestuur en de directeur houden toezicht op de werking van Europol. Voor het informatiebeheer beschikt Europol over het Europol-informatiesysteem, analysebestanden en Siena. Het Europol-informatiesysteem bevat persoonsgegevens, waaronder biometrische kenmerken, strafrechtelijke veroordelingen en gegevens over banden met georganiseerde criminaliteit, over personen die worden verdacht van strafbare feiten die onder de bevoegdheid van Europol vallen. Alleen de nationale Europol-eenheden, de verbindingsofficieren, gemachtigde personeelsleden van Europol en de directeur hebben toegang tot het Europol-informatiesysteeem. De analysebestanden worden aangemaakt ten behoeve van strafrechtelijke onderzoeken en bevatten gegevens over personen en andere informatie die de nationale eenheden erin opnemen. Verbindingsofficieren hebben wel toegang tot de analysebestanden, maar alleen de analisten van Europol mogen er gegevens in opnemen. Aan de hand van een index kunnen de nationale eenheden en de

---

60 Besluit 2009/371/JBZ van de Raad, PB L 121 van 15.5.2009, blz. 37; Verordening (EG) nr. 45/2001, PB L 8 van 12.12001, blz. 1; Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108 van de Raad van Europa van 28.1.1981 (verdrag nr. 108 van de Raad van Europa); Aanvullend protocol bij het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens inzake toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens (ETS nr. 181) van de Raad van Europa van 8.11.2001 (aanvullend protocol 181); Aanbeveling nr. R(87) 15 van het Comité van Ministers tot regeling van het gebruik van persoonsgegevens op politieel gebied, Raad van Europa, 17.9.1987 (politieaanbeveling).

61 Kaderbesluit 2008/977/JBZ van de Raad, PB L 350 van 30.12.2008, blz. 60.

62 Besluit van de Raad 2009/371/JBZ, PB L 121 van 15.5.2009, blz. 37, ter vervanging van de Overeenkomst op grond van artikel K.3 van het Verdrag betreffende de Europese Unie tot oprichting van een Europese Politiedienst, PB C 316 van 27.11.1995, blz. 2.

verbindingsofficieren nagaan of een analysebestand gegevens bevat die van belang zijn voor hun lidstaat. Voor het uitwisselen van gevoelige gegevens voor rechtshandhavingsdoeleinden maken de lidstaten steeds vaker gebruik van Siena, het beveiligde systeem van Europol. Europol mag gegevens en inlichtingen, met inbegrip van persoonsgegevens, verwerken voor de vervulling van zijn taken. De lidstaten mogen de gegevens uit de bestanden van Europol alleen gebruiken voor het voorkomen en bestrijden van ernstige grensoverschrijdende criminaliteit. Elke beperking die door de verstrekkende lidstaat wordt gesteld aan het gebruik van de gegevens, geldt ook voor andere gebruikers die die gegevens uit de Europol-bestanden opvragen. Europol mag ook persoonsgegevens uitwisselen met derde landen die een operationele overeenkomst met Europol hebben en een passend niveau van gegevensbescherming bieden. Europol mag gegevens bewaren zo lang als nodig is voor de vervulling van zijn taken. Analysebestanden mogen maximaal drie jaar worden bewaard; deze termijn kan worden verlengd met nog eens drie jaar. De verwerking van persoonsgegevens moet in overeenstemming zijn met de specifieke gegevensbeschermingsvoorschriften van het oprichtingsbesluit (Besluit 2009/371/JBZ), alsook met Verordening (EG) 45/2001, verdrag nr. 108 van de Raad van Europa, aanvullend protocol nr. 181 en de politieaanbeveling[63]. De bepalingen van Kaderbesluit 2008/977/JBZ van de Raad zijn van toepassing op de uitwisseling van persoonsgegevens tussen de lidstaten en Europol[64]. Een gemeenschappelijk controleorgaan, bestaande uit leden van de nationale controleorganen, houdt toezicht op de verwerking van persoonsgegevens door Europol en op de doorgifte van persoonsgegevens aan derden. Het gemeenschappelijk controleorgaan brengt regelmatig verslag uit aan het Europees Parlement en de Raad. Europol legt jaarlijks een verslag over zijn activiteiten ter goedkeuring voor aan de Raad en ter informatie aan het Europees Parlement.

De aanslagen van 11 september 2001 hebben niet alleen gevolgen gehad voor een aantal van de hierboven beschreven instrumenten, maar ook geleid tot de oprichting van **Eurojust**[65], het **justitieel samenwerkingsteam van de Europese Unie.** Eurojust is een EU-orgaan dat de coördinatie van onderzoek en vervolging in de lidstaten en de samenwerking tussen de bevoegde nationale autoriteiten moet verbeteren. Eurojust bestrijkt dezelfde soorten criminaliteit en strafbare feiten als Europol. Binnen die bevoegdheden hebben de 27 nationale leden van Eurojust, die samen het college vormen, voor de vervulling van hun taken toegang tot de persoonsgegevens van verdachten en veroordeelden. Daarbij gaat het onder andere om de volgende gegevens: biografische gegevens, contactgegevens, gegevens uit kentekenregisters, DNA-profielen, foto's, vingerafdrukken, alsmede verkeers- locatie- en abonneegegevens van aanbieders van telecommunicatiediensten. De lidstaten worden geacht dergelijke gegevens te delen met Eurojust om Eurojust in staat te stellen zijn taken te vervullen. Alle dossier-gerelateerde persoonsgegevens moeten in het casemanagementsysteem van Eurojust worden ingevoerd; dit systeem werkt via het s-Testa-

---

63 Besluit 2009/371/JBZ van de Raad, PB L 121 van 15.5.2009, blz. 37; Verordening (EG) nr. 45/2001, PB L 8 van 12.12001, blz. 1; Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108 van de Raad van Europa van 28.1.1981 (verdrag nr. 108 van de Raad van Europa); Aanvullend protocol bij het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens inzake toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens (ETS nr. 181) van de Raad van Europa van 8.11.2001 (aanvullend protocol 181); Aanbeveling nr. R(87) 15 van het Comité van Ministers tot regeling van het gebruik van persoonsgegevens op politieel gebied, Raad van Europa, 17.9.1987 (politieaanbeveling).

64 Kaderbesluit 2008/977/JBZ van de Raad, PB L 350 van 30.12.2008, blz. 60.

65 Besluit 2002/187/JBZ, PB L 63 van 6.3.2002, blz. 1. Besluit gewijzigd bij Besluit 2009/426/JBZ, PB L 138 van 4.6.2009, blz. 14. Zie ook de Buitengewone Raad Justitie en Binnenlandse zaken van 20.9.2001.

netwerk van de Commissie. Via een register worden persoonsgegevens en andere gegevens die van belang zijn voor lopende onderzoeken opgeslagen. Europol mag bij het vervullen van zijn taken persoonsgegevens verwerken, maar moet zich daarbij houden aan de specifieke voorschriften van zijn eigen oprichtingsbesluit (Besluit 2009/426/JBZ van de Raad) en aan verdrag nr. 108 van de Raad van Europa, het aanvullend protocol en de politieaanbeveling. De bepalingen van Kaderbesluit 2008/977/JBZ van de Raad zijn van toepassing op de uitwisseling van persoonsgegevens tussen de lidstaten en Eurojust[66]. Eurojust mag gegevens uitwisselen met nationale autoriteiten en derde landen waarmee het een overeenkomst heeft gesloten, mits het nationale lid dat de gegevens heeft verstrekt, instemt met de doorgifte ervan en het derde land een passend beschermingsniveau van persoonsgegevens biedt. Persoonsgegevens mogen worden bewaard zolang dat nodig is om de doelstellingen van Eurojust te verwezenlijken, maar moeten worden gewist zodra een dossier is afgesloten. De lidstaten moeten uiterlijk in juni 2011 voldoen aan de gewijzigde rechtsgrond van Eurojust. In juni 2014 moet de Commissie de uitwisseling van gegevens tussen de nationale leden van Eurojust evalueren en kan zij zo nodig wijzigingen voorstellen. In juni 2013 moet Eurojust verslag uitbrengen aan de Raad en de Commissie over de ervaringen met het verlenen van toegang tot het casemanagementsysteem op nationaal niveau. De lidstaten kunnen op basis daarvan hun nationale toegangsrechten herzien. Een gemeenschappelijk controleorgaan, bestaande uit door de lidstaten aangestelde rechters, houdt toezicht op de verwerking van persoonsgegevens door Eurojust en brengt jaarlijks verslag uit aan de Raad. De voorzitter van het college dient jaarlijks bij de Raad een verslag in over de activiteiten van Eurojust, dat door de Raad wordt doorgestuurd naar het Europees Parlement.

Internationale overeenkomsten ter voorkoming en bestrijding van terrorisme en andere vormen van ernstige grensoverschrijdende criminaliteit

Na de aanslagen van 11 september 2001 hebben de VS wetgeving vastgesteld die vliegtuigmaatschappijen die vluchten naar, vanuit of over het Amerikaanse grondgebied uitvoeren, verplicht de Amerikaanse autoriteiten persoonsgegevens van passagiers (**passenger name record** (PNR)) uit hun boekingssystemen te verstrekken. Canada en Australië volgden al snel. Omdat de desbetreffende EU-wetgeving vereist dat eerst het gegevensbeschermingsniveau in derde landen wordt beoordeeld, nam de Commissie de taak op zich om met deze landen onderhandelingen te voeren over PNR-overeenkomsten[67]. Zij heeft in juli 2007 de overeenkomst met de VS ondertekend, in juni 2008 die met Australië en in oktober 2005 een API/PNR-overeenkomst met Canada[68]. De overeenkomsten met de VS en Australië zijn voorlopig van toepassing, terwijl die met Canada van kracht blijft ondanks het feit dat de beschikking inzake het passende beschermingsniveau van persoonsgegevens in Canada in september 2009 is verlopen[69]. Het Europees Parlement stond kritisch tegenover deze overeenkomsten en heeft de Commissie opgeroepen over alle drie de overeenkomsten

---

66 Kaderbesluit 2008/977/JBZ van de Raad, PB L 350 van 30.12.2008, blz. 60.

67 Richtlijn 95/46/EG (Gegevensbeschermingsrichtlijn), PB L 281 van 23.11.1995, blz. 31.

68 Het Canadese pakket bestaat uit een verbintenis van Canada betreffende de verwerking van API/PNR-gegevens, de beschikking van de Commissie over de passende bescherming van persoonsgegevens in Canada en een internationale overeenkomst (zie PB L 91 van 29.3.2006, blz. 49, PB L 82 van 21.3.2006, blz. 14). De overeenkomst met de VS is te vinden in PB L 204 van 4.8. 2007, blz. 16, die met Australië in PB L 213 van 8.8.2008, blz. 47.

69 In 2009 is Canada jegens de Commissie, het voorzitterschap van de Raad en de EU-lidstaten de verbintenis aangegaan de eerdere verbintenis uit 2005 betreffende het gebruik van PNR-gegevens van de EU te blijven toepassen. De beschikking van de Commissie over het passende beschermingsniveau was op die eerdere verbintenis gebaseerd.

opnieuw te onderhandelen op basis van een reeks duidelijke beginselen[70]. PNR-gegevens worden ruim voor vertrek doorgegeven, zodat rechtshandhavingsautoriteiten ze kunnen gebruiken bij het screenen van passagiers op mogelijke banden met terrorisme of andere vormen van ernstige criminaliteit. Doel van elk van de overeenkomsten is dan ook het voorkomen en bestrijden van terrorisme en andere grensoverschrijdende vormen van ernstige criminaliteit. In ruil voor de PNR-gegevens uit de EU deelt het Amerikaanse ministerie van Binnenlandse Veiligheid (Department of Homeland Security, DHS) eventuele "aanwijzingen" die uit de PNR-analyse naar voren komen, met de rechtshandhavingsinstanties van de EU, met Europol en met Eurojust. Zowel Canada als de VS hebben in hun respectieve overeenkomsten toegezegd met de EU te zullen samenwerken wanneer zij haar eigen PNR-systeem opzet. De overeenkomsten met de VS en Australië bevatten 19 categorieën gegevens, waaronder biografische gegevens, boekingsgegevens, betalingsgegevens en aanvullende gegevens; de overeenkomst met Canada bevat 25 vergelijkbare categorieën. Onder de categorie aanvullende gegevens vallen onder andere gegevens over enkele reizen, standby-status en no-show-informatie. De overeenkomst met de VS laat, onder speciale voorwaarden, ook het gebruik van gevoelige informatie toe. Het DHS mag dergelijke gegevens verwerken indien het leven van de betrokkene of van anderen in gevaar is, maar moet ze binnen 30 dagen wissen. De PNR-gegevens worden naar een aantal centrale eenheden binnen het DHS, het Canada Border Services Agency en de Australian Customs Service gestuurd, die ze mogen doorgeven aan andere nationale autoriteiten die belast zijn met rechtshandhaving of terrorismebestrijding. In de overeenkomst met de VS staat dat het DHS verwacht dat het niet wordt verzocht voor de verwerking van PNR-gegevens uit de EU gegevensbeschermingsmaatregelen in zijn PNR-systeem in te voeren die strikter zijn dan die welke door Europese autoriteiten voor hun nationale PNR-systemen worden toegepast. Indien niet aan deze verwachting wordt voldaan, kan het DHS bepaalde onderdelen van de overeenkomst opschorten. Canada en Australië worden geacht een passend beschermingsniveau te bieden voor PNR-gegevens uit de EU als zij aan de voorwaarden van de overeenkomst voldoen. In de VS worden PNR-gegevens uit de EU zeven jaar bewaard in een actieve gegevensbank en daarna nog eens acht jaar in een slapende. In Australië worden ze voor drieënhalf jaar opgeslagen in een actieve gegevensbank en vervolgens twee jaar in een slapende. In beide landen is de slapende gegevensbank alleen toegankelijk met een speciale machtiging. In Canada worden de gegevens drieënhalf jaar bewaard, waarbij de gegevens na 72 uur anoniem worden gemaakt. Elk van de overeenkomsten voorziet in periodieke evaluaties en de overeenkomst met Canada en Australië bevat ook een beëindigingsclausule. In de EU beschikt alleen het Verenigd Koninkrijk over een PNR-systeem. Frankrijk, Denemarken, België, Zweden en Nederland hebben wetgeving op dit gebied vastgesteld of testen momenteel het gebruik van PNR-gegevens ter voorbereiding van het opzetten van een PNR-systeem. Ook andere lidstaten overwegen een PNR-systeem in te voeren en alle lidstaten maken in individuele gevallen gebruik van PNR-gegevens voor rechtshandhavingsdoeleinden.

Na de aanslagen van 11 september 2001 heeft het Amerikaanse ministerie van Financiën een programma voor het opsporen van de financiering van terroristische activiteiten vastgesteld, het **Terrorist Finance Tracking Program** (TFTP), voor het identificeren, opsporen en vervolgen van terroristen en hun geldschieters. In het kader van het TFTP werd het Amerikaanse filiaal van een Belgische onderneming door middel van een dwangbevel gedwongen een beperkt aantal gegevens betreffende het financiële berichtenverkeer dat over haar netwerk verliep, aan het Amerikaanse ministerie van Financiën door te geven. In januari

[70] Resolutie van het Europees Parlement P7_TA (2010)0144 van 5.5.2010.

2010 veranderde deze onderneming de architectuur van haar systeem, waardoor de hoeveelheid gegevens die onder Amerikaanse jurisdictie vallen en ten aanzien waarvan het ministerie van Financiën doorgaans een dwangbevel uitvaardigt, met meer dan de helft verminderde. In november 2009 hebben de voorzitter van de Raad van de Europese Unie en de regering van de Verenigde Staten een interim-overeenkomst ondertekend inzake de verwerking en doorgifte van gegevens betreffende het financiële berichtenverkeer van de EU naar de VS ten behoeve van het TFTP, die niet door het Parlement is goedgekeurd[71]. Op basis van een nieuw mandaat heeft de Europese Commissie met de VS onderhandeld over een nieuwe ontwerp-overeenkomst en op 18 juni 2010 bij de Raad een voorstel ingediend voor een besluit betreffende de sluiting van de overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en doorgifte van gegevens betreffende het financiële berichtenverkeer van de Europese Unie naar de Verenigde Staten ten behoeve van het Programma voor het traceren van terrorismefinanciering (EU-VS TFTP-overeenkomst)[72]. Het Europees Parlement heeft op 8 juli 2010 ingestemd met de sluiting van deze overeenkomst[73]. Nu moet de Raad een besluit vaststellen betreffende de sluiting van deze overeenkomst, waarna de overeenkomst in werking kan treden door middel van een briefwisseling tussen beide partijen. Doel van de EU-VS TFTP-overeenkomst is het voorkomen, onderzoeken, opsporen of vervolgen van terrorisme of terrorismefinanciering. De overeenkomst verplicht aangewezen verstrekkers van diensten betreffende het financiële berichtenverkeer om op basis van geografische dreigingsanalyses en op maat gesneden verzoeken gegevens betreffende het financiële berichtenverkeer, zoals naam, rekeningnummer, adres en identificatienummer van de opdrachtgever en ontvanger(s) van financiële transacties, te verstrekken aan het Amerikaanse ministerie van Financiën. Het ministerie van Financiën mag deze gegevens uitsluitend doorzoeken ten behoeve van het TFTP en alleen als er reden is om aan te nemen dat bij een bepaalde persoon sprake is van een verband met terrorisme of terrorismefinanciering. Datamining en de doorgifte van gegevens betreffende transacties binnen de eengemaakte eurobetalingsruimte zijn verboden. De VS geeft eventuele "aanwijzingen" over terroristische aanslagen die mogelijk in de EU worden beraamd door aan de EU-lidstaten, Europol en Eurojust, en helpt de EU bij het opzetten van een eigen systeem dat vergelijkbaar is met het TFTP. Indien de EU een dergelijk programma opstelt, kunnen beide partijen de voorwaarden van de overeenkomst aanpassen. Voordat er gegevens kunnen worden doorgegeven, moet voor elk verzoek van de VS door Europol worden nagegaan of het voldoet aan de voorwaarden van de overeenkomst. Informatie die uit verstrekte gegevens over het financiële berichtenverkeer wordt geëxtraheerd, mag niet langer worden bewaard dan noodzakelijk is voor het specifieke onderzoek of de specifieke vervolging waarvoor ze wordt gebruikt; niet-geëxtraheerde gegevens mogen vijf jaar worden bewaard. Indien dit noodzakelijk is voor het onderzoeken, voorkomen of vervolgen van terrorisme of terrorismefinanciering, mag het ministerie van Financiën persoonsgegevens die het uit het financiële berichtenverkeer heeft geëxtraheerd, doorgeven aan de Amerikaanse rechtshandavings-, openbareveiligheids- of terrorismebestrijdingsautoriteiten, aan Europol en aan Eurojust. Het mag ook aanwijzingen betreffende EU-onderdanen en –ingezetenen delen met derde landen, mits de betrokken lidstaat daarmee instemt. Op de naleving van de strikte beperking van het doel tot de bestrijding van terrorisme en de inachtneming van de andere waarborgen wordt toezicht gehouden door onafhankelijke toezichthouders, onder wie een door de Commissie aangewezen persoon. De overeenkomst heeft een looptijd van vijf jaar en kan worden beëindigd of opgeschort door elk van beide partijen. Een evaluatieteam van de

---

71 Resolutie van het Europees Parlement P7_TA (2010)0029 van 11.2.2010.

72 COM(2010)316 definitief/2 van 18.6.2010

73 Resolutie van het Europees Parlement, P7-TA-PROV(2010)0279 van 8.7.2010.

EU, onder leiding van de Commissie en bestaande uit vertegenwoordigers van twee gegevensbeschermingsinstanties en een persoon met een juridische achtergrond, evalueert deze overeenkomst zes maanden na de inwerkingtreding ervan, waarbij in het bijzonder aandacht wordt besteed aan de toepassing van de doelbindings- en evenredigheidsbepalingen en aan de naleving van de gegevensbeschermingsverplichtingen. Het verslag van de Commissie zal aan het Europees Parlement en de Raad worden voorgelegd.

2.2. Initiatieven in het kader van het actieplan ter uitvoering van het programma van Stockholm

Wetgevingsvoorstellen die door de Commissie moeten worden ingediend

In het programma van Stockholm heeft de Europese Raad de Commissie verzocht drie voorstellen in te dienen die van direct belang zijn voor deze mededeling: een voorstel betreffende een EU-PNR-systeem voor het voorkomen, opsporen en vervolgen van terrorisme en ernstige criminaliteit, een voorstel voor een inreis/uitreis-systeem, en een voorstel betreffende een programma voor geregistreerde reizigers. De laatste twee zouden volgens de Europese Raad zo snel mogelijk moeten worden ingediend. De Commissie heeft alle drie de verzoeken opgenomen in haar actieplan ter uitvoering van het programma van Stockholm[74]. Zij werkt er nu aan gevolg te geven aan deze verzoeken en zal in de toekomst deze instrumenten evalueren op basis van de beleidsontwikkelingsbeginselen die zijn geformuleerd in punt 4.

In november 2007 heeft de Commissie een voorstel ingediend voor een kaderbesluit van de Raad over het gebruik van PNR-gegevens voor rechtshandhavingsdoeleinden[75]. Dit initiatief werd gesteund door de Raad en werd vervolgens gewijzigd om rekening te houden met de wijzigingen die door het Europees Parlement waren voorgesteld en met het standpunt van de Europese Toezichthouder voor gegevensbescherming. Met de inwerkingtreding van het Verdrag van Lissabon kwam het voorstel te vervallen. Zoals gepland in het actieplan ter uitvoering van het programma van Stockholm werkt de Commissie nu aan een **Passenger Name Record-pakket** dat begin 2011 moet worden ingediend en dat het volgende omvat: een mededeling over een externe PNR-strategie waarin de basisbeginselen voor onderhandelingen over overeenkomsten met derde landen uiteen worden gezet, onderhandelingsrichtsnoeren voor de nieuwe onderhandelingen over een PNR-overeenkomst met de VS en met Australië, en onderhandelingsrichtsnoeren voor een nieuwe overeenkomst met Canada. Tevens werkt de Commissie aan een nieuw EU-PNR-voorstel.

In 2008 heeft de Commissie een aantal suggesties gedaan voor de ontwikkeling van het geïntegreerde grensbeheer door het reizen voor onderdanen van derde landen te vergemakkelijken en tegelijkertijd de interne veiligheid te verbeteren[76]. Omdat personen die de toegestane verblijfsduur overschrijden de grootste groep onregelmatige migranten in de EU vormen, heeft de Commissie voorgesteld eventueel een **inreis-/uitreissystem** in te voeren voor onderdanen van derde landen die voor een kort verblijf van maximaal drie maanden naar de EU komen. Met een dergelijk systeem zouden tijd en plaats van inreis en de toegestane verblijfsduur worden geregistreerd en zou automatisch een signaal naar de bevoegde

---

74 Het programma van Stockholm - Een open en veilig Europa ten dienste en ter bescherming van de burger, Raadsdocument 5731/10 van 3.3.2010, COM(2010)171 van 20.4.2010 (Actieplan ter uitvoering van het programma van Stockholm).

75 COM(2007) 654 van 6.11.2007.

76 COM(2008) 69 van 13.2.2008.

instanties worden gestuurd waarmee wordt aangegeven welke personen de toegestane verblijfsduur hebben overschreden. Het systeem zou met hetzelfde biometrische matchingsysteem en dezelfde apparatuur werken als SIS II en VIS. De Commissie verricht momenteel een effectbeoordeling en streeft ernaar, volgens de planning van het actieplan ter uitvoering van het programma van Stockholm in 2011 met een wetgevingsvoorstel te komen.

Het derde voorstel betreft een **programma voor geregistreerde reizigers**[77]. Dit programma zou bepaalde groepen frequente bezoekers uit derde landen de mogelijkheid bieden om, na een voorafgaande controleprocedure, via vereenvoudigde grenscontroles aan automatische poorten de EU binnen te komen. Het programma zou zijn gebaseerd op identiteitscontroles door middel van biometrische gegevens en zou het mogelijk maken geleidelijk over te schakelen van de bestaande algemene grenscontrole naar een controlesysteem op basis van individuele risico's. De Commissie heeft een effectbeoordeling verricht en streeft ernaar, volgens de planning van het actieplan ter uitvoering van het programma van Stockholm in 2011 met een wetgevingsvoorstel te komen.

Initiatieven die door de Commissie moeten worden bestudeerd

In het programma van Stockholm heeft de Europese Raad de Commissie verzocht drie initiatieven te bestuderen die van belang zijn voor deze mededeling: de mogelijkheden onderzoeken voor het traceren van terrorismefinanciering binnen de EU, onderzoeken of het mogelijk en nuttig is een Europees systeem voor reisvergunningen te ontwikkelen, en een studie te verrichten naar de behoefte aan en de toegevoegde waarde van het opzetten van een Europees Indexsysteem van politiegegevens. De Commissie heeft ook deze drie initiatieven opgenomen in haar actieplan ter uitvoering van het programma van Stockholm. Zij zal zich nu buigen over de haalbaarheid ervan en besluiten of en hoe zij deze initiatieven zal uitwerken, op basis van de beleidsontwikkelingsbeginselen die zijn geformuleerd in punt 4.

De EU-VS TFTP-overeenkomst bepaalt dat de Europese Commissie een studie moet uitvoeren naar de mogelijke invoering van een **EU-systeem voor het traceren van terrorismefinanciering**, vergelijkbaar met het Amerikaanse TFTP, om een meer gerichte doorgifte van gegevens mogelijk te maken. In het voorstel voor een besluit van de Raad over de sluiting van deze overeenkomst wordt de Commissie tevens verzocht uiterlijk een jaar na de datum van inwerkingtreding van de overeenkomst een juridisch en technisch kader voor het extraheren van gegevens op het EU-grondgebied voor te leggen aan het Europees Parlement en de Raad[78]. Uiterlijk drie jaar na de inwerkingtreding van de overeenkomst moet de Commissie een voortgangsverslag indienen over de ontwikkeling van een dergelijk EU-systeem. Indien het soortgelijke EU-systeem vijf jaar na de datum van inwerkingtreding van de overeenkomst niet tot stand is gebracht, kan de EU besluiten de overeenkomst te beëindigen. De EU-VS TFTP-overeenkomst verplicht de VS om, indien de Europese Unie besluit een EU-systeem in te stellen, daaraan mee te werken en assistentie en advies te verlenen. Zonder vooruit te lopen op een eventueel besluit, is de Commissie begonnen de gegevensbeschermingsaspecten, de consequenties voor de middelen en de praktische implicaties van deze stap te analyseren. Zoals aangekondigd in het actieplan ter uitvoering van het programma van Stockholm, zal de Commissie in 2011 met een mededeling komen over de haalbaarheid van een EU-programma voor het traceren van terrorismefinanciering (EU-TFTP).

---

77 COM(2008) 69 van 13.2.2008.

78 Raadsdocument 11222/1/10 REV 1 van 24.6.2010.

In haar mededeling van 2008 over het geïntegreerd grensbeheer heeft de Commissie de suggestie gedaan een **elektronisch systeem voor reisvergunningen** in te voeren voor niet-visumplichtige onderdanen van derde landen[79]. Dit programma zou inhouden dat onderdanen van derde landen die hiervoor in aanmerking komen, zou worden verzocht vóór vertrek een elektronische aanvraag in te dienen en hierin zowel informatie ter identificatie van de reiziger als paspoort- en reisgegevens te verschaffen. In vergelijking met de visumprocedure zou met dit systeem sneller en eenvoudiger kunnen worden gecontroleerd of een persoon aan de inreisvoorwaarden voldoet. De Commissie voert momenteel een studie uit naar de voor- en nadelen en de praktische implicaties van de invoering van het elektronisch systeem. Zoals aangekondigd in het actieplan ter uitvoering van het programma van Stockholm, streeft de Commissie ernaar in 2011 een mededeling te presenteren over de haalbaarheid van een dergelijk systeem.

Tijdens zijn voorzitterschap van de Raad in 2007 heeft Duitsland een discussie op gang gebracht over de mogelijke invoering van een **Europees Indexsysteem van politiegegevens** (Epris)[80]. Epris zou rechtshandhavingsambtenaren moeten helpen gegevens in de EU te lokaliseren, in het bijzonder gegevens betreffende de verbanden tussen personen die ervan worden verdacht betrokken te zijn bij georganiseerde criminaliteit. De Commissie zal in 2010 een ontwerpopdracht voor de haalbaarheidsstudie over Epris voorleggen aan de Raad. Zoals aangekondigd in het actieplan ter uitvoering van het programma van Stockholm, streeft de Commissie ernaar in 2012 een mededeling te presenteren over de haalbaarheid van een dergelijk systeem.

3. ANALYSE VAN DE INSTRUMENTEN DIE AL WORDEN GEBRUIKT, DIE NU WORDEN INGEVOERD OF WAAROVER NU WORDT GESPROKEN

Het hierboven geschetste overzicht levert de volgende voorlopige bevindingen op:

Gedecentraliseerde structuur

Van de verschillende instrumenten die momenteel in gebruik zijn, die nu worden ingevoerd of waarover wordt gesproken, zijn er maar zes waarbij persoonsgegevens op EU-niveau worden verzameld of opgeslagen: SIS (en SIS II), VIS, Eurodac, DIS, Europol en Eurojust. Alle andere maatregelen regelen de gedecentraliseerde, grensoverschrijdende uitwisseling of doorgifte van persoonsgegevens die op nationaal niveau zijn verzameld door overheidsinstanties of particuliere ondernemingen. De meeste persoonsgegevens worden op nationaal niveau verzameld en opgeslagen; de EU wil een meerwaarde bieden door onder bepaalde voorwaarden de uitwisseling van dergelijke gegevens met EU-partners en derde landen mogelijk te maken. De Commissie heeft onlangs bij het Europees Parlement en de Raad een gewijzigd voorstel ingediend tot oprichting van een agentschap voor het operationele beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht[81]. Het toekomstige IT-agentschap moet het operationele beheer van SIS II, VIS en Eurodac en van alle andere toekomstige IT-systemen op het gebied van vrijheid, veiligheid en recht op zich nemen en ervoor zorgen dat deze systemen permanent blijven werken, zodat een ononderbroken informatiestroom is gewaarborgd.

---

79 COM(2008) 69 van 13.2.2008.

80 Raadsdocument 15526/1/09 van 2.12.2009.

81 COM(2010) 93 van 19.3.2010.

Beperkt doel

De meeste van de hierboven beschreven instrumenten hebben een enkelvoudig doel: Eurodac moet de werking van het Dublinsysteem verbeteren, API moet de grenscontrole bevorderen, het Zweedse initiatief moet leiden tot efficiëntere strafrechtelijke onderzoeken en inlichtingenoperaties, de Napels II-overeenkomst moet douanefraude helpen voorkomen, opsporen, vervolgen en bestraffen, het DIS moet helpen bij het voorkomen, onderzoeken en vervolgen van ernstige schendingen van nationale wetten door middel van een doeltreffender samenwerking tussen nationale douanediensten, het Ecris, de FIE's en de bureaus voor de ontneming van vermogensbestanddelen moeten de grensoverschrijdende uitwisseling van gegevens op bepaalde gebieden stroomlijnen, en het Prümbesluit, de richtlijn gegevensbewaring, TFTP en PNR moeten terrorisme en ernstige criminaliteit bestrijden. SIS, SIS II en VIS zijn kennelijk de belangrijkste uitzonderingen op deze regel: oorspronkelijk was het VIS bedoeld om de grensoverschrijdende uitwisseling van visumgegevens te vergemakkelijken, maar later werd dit doel uitgebreid tot het voorkomen en bestrijden van terrorisme en ernstige criminaliteit. SIS en SIS II zijn bedoeld om een hoog niveau van veiligheid in de ruimte van vrijheid, veiligheid en recht te garanderen en het personenverkeer te bevorderen aan de hand van de gegevens die via dit systeem worden verwerkt. Met uitzondering van deze gecentraliseerde informatiesystemen, lijkt doelbeperking een kernelement te zijn bij het uitwerken van EU-maatregelen op het gebied van informatiebeheer.

Potentiële overlappingen

Dezelfde persoonsgegevens kunnen via verschillende instrumenten worden verzameld, maar mogen in het kader van een bepaald instrument alleen worden gebruikt voor een specifiek doel (behalve in het geval van VIS, SIS en SIS II). Zo kunnen de biografische gegevens zoals naam, geboortedatum en –plaats en nationaliteit worden verwerkt via SIS, SIS II, VIS, API, DIS, het Zweedse initiatief, het Prümbesluit, Ecris, FIE's, bureaus voor de ontneming van vermogensbestanddelen, Europol, Eurojust en de PNR- en TFTP-overeenkomsten. Deze gegevens mogen in het kader van de API echter uitsluitend worden verwerkt voor de grenscontrole, in het kader van het DIS voor het voorkomen, onderzoeken en vervolgen van douanefraude, in het kader van het Zweedse initiatief voor strafrechtelijke onderzoeken en inlichtingenoperaties, in het kader van het Prümbesluit voor het voorkomen van terrorisme en grensoverschrijdende criminaliteit, in het kader van het Ecris voor het onderzoeken van iemands criminele achtergrond, in het kader van de FIE's voor het onderzoeken van de banden die iemand heeft met georganiseerde criminele en terroristische netwerken, in het kader van de bureaus voor de ontneming van vermogensbestanddelen voor het traceren van vermogensbestanddelen, in het kader van Europol en Eurojust voor het onderzoeken en helpen vervolgen van ernstige grensoverschrijdende criminaliteit, in het kader van de PNR-overeenkomsten voor het voorkomen en bestrijden van terrorisme en andere vormen van ernstige criminaliteit, en in het kader van het TFTP voor het identificeren en vervolgen van terroristen en hun geldschieters. Biometrische gegevens zoals vingerafdrukken en foto's mogen worden verwerkt via SIS II, VIS, Eurodac, het Zweedse initiatief, het Prümbesluit, het Ecris, Europol en Eurojust – maar ook in dit geval alleen voor het specifieke doel van elk afzonderlijk instrument. Het Prümbesluit is het enige instrument dat de grensoverschrijdende uitwisseling van anonieme DNA-profielen mogelijk maakt (hoewel dergelijke gegevens ook aan Europol en Eurojust mogen worden doorgegeven). In het kader van andere instrumenten wordt met zeer specifieke persoonsgegevens gewerkt die relevant zijn voor het doel van het instrument: in PNR-systemen met boekingsgegevens van vliegtuigpassagiers, in het FIDE met gegevens die van belang zijn voor het onderzoeken van douanefraude, in het kader van de

richtlijn gegevensbewaring met IP-adressen en identificatiecodes voor mobiele apparatuur, in het Ecris met gegevens uit het strafregister, in bureaus voor de ontneming van vermogensbestanddelen met gegevens over particuliere vermogens en ondernemingen, in cybercriminaliteitplatforms met inbreuken op internet, bij Europol met banden met criminele netwerken, en in het TFTP met gegevens betreffende het financiële berichtenverkeer. De enige echte overlapping hierbij is de grensoverschrijdende uitwisseling van gegevens en inlichtingen voor strafrechtelijke onderzoeken. Uit juridisch oogpunt zou het Zweedse initiatief voldoende grond bieden voor het uitwisselen van elke vorm van informatie die van belang is voor dergelijke onderzoeken (mits de uitwisseling van dergelijke persoonsgegevens is toegestaan volgens nationaal recht). Uit operationeel oogpunt kunnen DNA-profielen en vingerafdrukken echter het best op basis van het Prümbesluit worden uitgewisseld, omdat het hit/no hit-systeem onmiddellijk een antwoord oplevert en de geautomatiseerde gegevensuitwisselingsmethode een hoog niveau van gegevensbeveiliging biedt[82]. Evenzo kan het voor FIE's, bureaus voor de ontneming van vermogensbestanddelen en cybercriminaliteitplatforms efficiënter zijn om rechtstreeks contact op te nemen met hun EU-collega's zonder de formulieren in te vullen die moeten worden gebruikt als op grond van het Zweedse initiatief gegevens worden opgevraagd.

Gecontroleerde toegang

De toegang tot instrumenten die zijn bedoeld voor de bestrijding van terrorisme en ernstige criminaliteit is doorgaans beperkt tot rechtshandhavingsinstanties in engere zin, namelijk politie, grenswacht en douane. Bij maatregelen die voortkomen uit de Schengengedachte zijn het meestal de immigratieautoriteiten en in bepaalde omstandigheden ook de politie, de grenswacht en de douane die toegang hebben. Bij SIS en VIS wordt de informatiestroom gestuurd door nationale interfaces en bij de gedecentraliseerde instrumenten door nationale contactpunten of centrale coördinatie-eenheden, zoals bij het Prümbesluit, het Zweedse initiatief, de Napels II-overeenkomst, het Ecris, het TFTP, de PNR-overeenkomsten, de FIE's, de bureaus voor de ontneming van vermogensbestanddelen en de cybercriminaliteitplatforms.

Uiteenlopende regels voor de bewaring van de gegevens

De bewaartermijnen lopen sterk uiteen naar gelang van de doelstellingen van de verschillende instrumenten. De PNR-overeenkomst met de VS kent de langste bewaartermijn: 15 jaar; de API de kortste: 24 uur. In de PNR-overeenkomsten wordt een interessant onderscheid ingevoerd tussen actieve en slapende gegevensbanken: na een bepaalde periode moeten gegevens worden gearchiveerd en kunnen ze alleen met een speciale machtiging worden "ontsloten". De manier waarop Canada de PNR-gegevens van de EU gebruikt, is daar een goed voorbeeld van: de gegevens moeten na 72 uur anoniem worden gemaakt, maar blijven gedurende drieënhalfjaar beschikbaar voor gemachtigde ambtenaren.

Effectief identiteitsbeheer

Een aantal van de hierboven geanalyseerde instrumenten, zoals het toekomstige SIS II en VIS, maken identiteitscontrole aan de hand van biometrische gegevens mogelijk. De invoering van

---

[82] Bij het Prümbesluit (Besluit 2008/615/JBZ van de Raad, PB L 210 van 6.8.2008, blz. 1) hoort ook een uitvoeringsbesluit (Besluit 2008/615/JBZ van de Raad, PB L 210 van 6.8.2008, blz. 12), dat ervoor moet zorgen dat gebruikgemaakt wordt van geavanceerde technologie voor de bescherming en beveiliging van gegevens, en van versleuteling en autorisatieprocedures voor de toegang tot de gegevens; dit uitvoeringsbesluit bevat ook regels voor de toelaatbaarheid van bevragingen.

SIS II zal naar verwachting de veiligheid in de ruimte van vrijheid, veiligheid en recht verhogen doordat personen tegen wie bijvoorbeeld een Europees aanhoudingsbevel is uitgevaardigd, personen die niet mogen worden toegelaten tot het Schengengebied, of personen die om andere redenen worden gezocht (vermiste personen of getuigen) gemakkelijker kunnen worden geïdentificeerd, ongeacht de beschikbaarheid of de echtheid van de identiteitsdocumenten. De invoering van het VIS zal de visumafgifte en het visumbeheer vergemakkelijken.

Gegevensbeveiliging via EU-oplossingen

Voor het uitwisselen van gevoelige informatie over de Europese grenzen maken de lidstaten bij voorkeur gebruik van EU-oplossingen. Verschillende instrumenten, uiteenlopend qua omvang, structuur en doel, maken gebruik van het door de Commissie gefinancierde s-Testa-communicatienetwerk voor het uitwisselen van gevoelige gegevens. Dat geldt voor de gecentraliseerde systemen SIS II, VIS en Eurodac, de gedecentraliseerde instrumenten Prüm, Ecris en FIE, en voor Europol en Eurojust. Het DIS en het FIDE maken gebruik van het gemeenschappelijk communicatienetwerk, de gemeenschappelijke systeeminterface of de beveiligde internettoegang van de Commissie. Daarentegen lijkt het beveiligde gegevensuitwisselingssysteem Siena van Europol de voorkeursoptie te zijn bij een aantal recente initiatieven waarbij beveiligde gegevensoverdracht nodig is: er zijn besprekingen gaande om fiu.net, de bureaus voor de ontneming van vermogensbestanddelen en de cybercriminaliteitplatforms te laten werken via deze toepassing.

Uiteenlopende evaluatiemechanismen

De evaluatiemechanismen van de hierboven beschreven instrumenten lopen nogal uiteen. Voor complexe systemen zoals SIS II, VIS en Eurodac moet de Commissie jaarlijks of haljaarlijks bij het Europees Parlement en de Raad een verslag indienen over de werking of de vorderingen bij de invoering van deze systemen. Bij de gedecentraliseerde informatie-uitwisselingsinstrumenten moet de Commissie enkele jaren na de inwerkingtreding van het instrument een evaluatieverslag voorleggen aan de andere instellingen: de richtlijn gegevensbewaring, het Zweedse initiatief en de bureaus voor de ontneming van vermogensbestanddelen moeten worden geëvalueerd in 2010, het Prümbesluit in 2012 en het Ecris in 2016. De drie PNR-overeenkomsten voorzien in periodieke en ad-hoc-evaluaties, en twee van de drie ook in een vervalbepaling. Europol en Eurojust dienen jaarlijks een verslag in bij de Raad, die dit ter informatie doorstuurt naar het Europees Parlement. Hieruit blijkt dat de huidige structuur van het informatiebeheer in de EU zich niet leent voor één enkel evaluatiemechanisme voor alle instrumenten. Gezien deze diversiteit is het van wezenlijk belang dat bij toekomstige wijzigingen van een informatiebeheersinstrument rekening wordt gehouden met de potentiële gevolgen voor alle andere maatregelen die het verzamelen, opslaan of uitwisselen van persoonsgegevens op het gebied van vrijheid, veiligheid en recht regelen.

4. BELEIDSONTWIKKELINGSBEGINSELEN

In punt 2 worden verschillende instrumenten beschreven die de Europese Commissie de afgelopen jaren heeft ingevoerd, voorgesteld, of besproken. Het grote aantal nieuwe ideeën en het groeiende wetgevingscorpus op het gebied van interne veiligheid en migratiebeheer maken het noodzakelijk een reeks basisbeginselen vast te stellen die de komende jaren als uitgangspunt moeten dienen bij het formuleren en evalueren van beleidsvoorstellen. Deze

beginselen zijn een voortvloeisel en een aanvulling van de algemene beginselen die zijn vastgelegd in de EU-verdragen, de jurisprudentie van het Europese Hof van Justitie en het Europese Hof voor de rechten van de mens, en de desbetreffende interinstitutionele overeenkomsten tussen het Europees Parlement, de Raad en de Europese Commissie. De Commissie stelt voor bij het ontwikkelen en uitvoeren van nieuwe initiatieven en bij het evalueren van bestaande instrumenten uit te gaan van de twee reeksen beginselen die hieronder worden beschreven.

Materiële beginselen

Waarborging van de grondrechten, in het bijzonder het recht op privacy- en gegevensbescherming

Het waarborgen van de grondrechten die zijn verankerd in het Handvest van de Grondrechten van de Europese Unie, in het bijzonder het recht op privacy- en gegevensbescherming, moet voor de Commissie voorop staan bij het formuleren van nieuwe voorstellen op het gebied van interne veiligheid of migratiebeheer die de verwerking van persoonsgegevens met zich brengen. De artikelen 7 en 8 van het handvest stellen dat eenieder recht heeft op "eerbiediging van zijn privéleven en zijn familie- en gezinsleven" en op "bescherming van de hem betreffende persoonsgegevens"[83]. Artikel 16 van het Verdrag betreffende de werking van de Europese Unie (VWEU), dat verbindend is voor de lidstaten, de instellingen en de organen van de Europese Unie, bevestigt het recht van eenieder op "bescherming van zijn persoonsgegevens"[84]. Nieuwe instrumenten waarin gebruik wordt gemaakt van informatietechnologie moeten worden ontwikkeld met "ingebouwde privacy" ("privacy by design"). Dit houdt in dat gegevensbescherming wordt ingebouwd in de technologische basis van een voorgesteld instrument, waardoor alleen gegevens worden verwerkt die nodig zijn voor een bepaald doel en toegang alleen wordt verleend op "need to know" basis[85].

Noodzakelijkheid

Inmenging in het recht op privacy door het openbaar gezag is soms noodzakeljk in het belang van de nationale veiligheid, de openbare veiligheid of het voorkomen van strafbare feiten[86]. Het Europees Hof voor de rechten van de mens heeft in zijn jurisprudentie drie voorwaarden gesteld waaronder deze beperking gerechtvaardigd kan zijn: zij moet wettig zijn, een legitiem doel nastreven en noodzakelijk zijn in een democratische samenleving. Beperking van het recht op privacy wordt noodzakelijk geacht als er sprake is van een dwingende maatschappelijke behoefte, als de beperking evenredig is aan het nagestreefde legitieme doel en als de redenen die de overheid voor de beperking opgeeft, relevant en toereikend zijn[87]. Bij alle toekomstige beleidsvoorstellen moet de Commissie nagaan wat het verwachte effect is van het initiatief op het recht op privacy- en gegevensbescherming en aangeven waarom dit effect noodzakelijk is en waarom de voorgestelde oplossing evenredig is met het legitieme

---

83 Handvest van de grondrechten van de Europese Unie, PB C 83 van 30.3.2010, blz. 389.

84 Geconsolideerde versies van het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie, PB C 83 van 30.3.2008, blz. 1.

85 Voor een uitvoerige beschrijving van "ingebouwde privacy" zie het advies van de Europese Toezichthouder voor gegevensbescherming over het bevorderen van vertrouwen in de informatiemaatschappij: "Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy" van 18.3.2010.

86 Zie artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (ETS nr. 5) van de Raad van Europa van 4.11.1950.

87 Zie *Marper v Unitd Kingdom*, Europees Hof voor de rechten van de mens, Straatsburg, 4.12.2008.

doel de interne veiligheid in de Europese Unie te handhaven, criminaliteit te voorkomen of de migratie te beheersen. In alle gevallen moet door een onafhankelijke autoriteit op nationaal of EU-niveau worden gecontroleerd of de regels inzake de bescherming van persoonsgegevens worden nageleefd.

Subsidiariteit

De Commissie moet haar nieuwe voorstellen toetsen aan het subsidiariteits- en het evenredigheidsbeginsel, overeenkomstig artikel 5 van protocol nr. 2 bij het Verdrag betreffende de Europese Unie. Elk nieuw wetgevingsvoorstel moet een verklaring bevatten op basis waarvan kan worden beoordeeld of het voorstel strookt met het subsidiariteitsbeginsel dat is vastgelegd in artikel 5 van het Verdrag betreffende de Europese Unie. Deze verklaring moet een beoordeling bevatten van de financiële, economische en sociale effecten en, in het geval van een richtlijn, van het effect ten aanzien van de regels die de lidstaten moeten invoeren[88]. De argumenten voor de conclusie dat een EU-doelstelling beter kan worden verwezenlijkt op EU-niveau moeten met kwalitatieve indicatoren worden ondersteund. In wetgevingsvoorstellen moet er rekening mee worden gehouden dat alle lasten voor de Unie, de nationale regeringen, de regionale overheden, het bedrijfsleven en de burgers tot een minimum moeten worden beperkt en in verhouding moeten staan tot het te bereiken doel. Als het gaat om voorstellen voor nieuwe internationale overeenkomsten wordt in deze verklaring ingegaan op de verwachte effecten van het voorstel op de betrekkingen met de betrokken derde landen.

Gericht risicobeheer

Gegevens op het gebied van vrijheid, veiligheid en recht worden meestal uitgewisseld om bedreigingen van de veiligheid te analyseren, trends in criminele activiteiten te signaleren of risico's op aanverwante beleidsterreinen te beoordelen[89]. Risico's houden vaak, maar niet altijd, verband met personen van wie het gedrag of het gedragspatroon in het verleden wijst op een voortdurend risico voor de toekomst. Risicobeoordeling moet echter zijn gebaseerd op bewijzen en niet op hypotheses. Noodzakelijkheidstoetsing en doelbinding zijn van wezenlijk belang voor elke maatregel op het gebied van informatiebeheer. Risicoprofielen – niet te verwarren met tegen de grondrechten indruisende raciale of anderszins discriminerende profilering – zijn nuttig. Dergelijke profielen kunnen er mede voor zorgen dat bepaalde middelen gericht worden ingezet voor specifieke personen teneinde veiligheidsdreigingen te beoordelen en slachtoffers van criminaliteit te beschermen.

Procesgerichte beginselen[90]

Kosteneffectiviteit

Overheidsdiensten die op informatietechnologie zijn gebaseerd moeten leiden tot een betere dienstverlening en ervoor zorgen dat de belastingbetaler meer waar voor zijn geld krijgt.

---

88 De basisbeginselen voor effectbeoordelingen zijn geformuleerd in de richtsnoeren voor effectbeoordeling van de Europese Commissie (SEC(2009)92 van 15.1.2009)

89 Praktische voorbeelden van geslaagd risicobeheer: voorkomen dat een persoon die in een lidstaat een ernstig misdrijf heeft gepleegd en het land is uitgezet, de Schengenruimte opnieuw binnenkomt via een andere lidstaat (SIS), of voorkomen dat iemand in verschillende lidstaten asiel aanvraagt (Eurodac).

90 Deze beginselen zijn gebaseerd op de conclusies van de Raad over een strategie voor het beheer van rechtshandhavingsinformatie voor interne veiligheid in de EU, Raad Justitie en Binnenlandse Zaken van 30.11.2009.

Gezien het huidige economische klimaat moeten alle nieuwe voorstellen, met name wanneer zij betrekking hebben op de invoering of aanpassing van informatiesystemen, zo kosteneffectief mogelijk zijn. Deze benadering houdt in dat rekening wordt gehouden met reeds bestaande systemen, om zo min mogelijk overlapping en zo veel mogelijk synergie te creëren. De Commissie moet beoordelen of de doelstellingen van een voorstel niet kunnen worden verwezenlijkt door bestaande instrumenten beter te gebruiken. Zij moet ook overwegen extra functies toe te voegen aan bestaande informatiesystemen voordat nieuwe systemen worden voorgesteld.

Bottom-up beleidsontwikkeling

Bij de ontwikkeling van nieuwe initiatieven moeten alle betrokkenen, zoals de nationale autoriteiten die het initiatief moeten uitvoeren, economische actoren en het maatschappelijk middenveld, vanaf een zo vroeg mogelijk stadium een inbreng hebben. Het ontwikkelen van beleid waarin rekening wordt gehouden met de belangen van de eindgebruikers vergt horizontaal denken en brede raadpleging[91]. Daarom moet de Commissie permanent contact proberen te onderhouden met nationale ambtenaren en praktijkmensen via de structuren van de Raad, beheerscomités en ad-hoc-overlegorganen.

Duidelijke verdeling van verantwoordelijkheden

Omdat de projecten voor het verzamelen en uitwisselen van gegevens op het gebied van vrijheid, veiligheid en recht technisch zeer complex zijn, verdient de beheerstructuur vanaf het begin bijzondere aandacht. De ervaring met het SIS II-project leert dat het ontbreken van een duidelijke en stabiele beschrijving van overkoepelende doelstellingen, taken en verantwoordelijkheden in het beginstadium, kan leiden tot aanzienlijke kostenoverschrijdingen en vertragingen bij de invoering. Uit de eerste ervaringen met het Prümbesluit blijkt echter dat een gedecentraliseerde beheerstructuur ook geen wondermiddel is, omdat er dan geen projectleider is tot wie de lidstaten zich kunnen wenden voor advies over de financiële of technische aspecten van de tenuitvoerlegging. Wellicht kan het toekomstige IT-agentschap beheerders van informatiesystemen op het gebied van vrijheid, veiligheid en recht technisch advies geven. Het kan tevens een platform bieden voor alle partijen die betrokken zijn bij het operationele beheer en de ontwikkeling van IT-systemen. Als mogelijke waarborg tegen kostenoverschrijdingen en vertragingen ten gevolge van veranderende eisen, mogen geen nieuwe informatiesystemen op het gebied van vrijheid, veiligheid en recht worden ontwikkeld, zeker niet als het gaat om een grootschalig IT-systeem, voordat de desbetreffende rechtsinstrumenten waarin het doel, het toepassingsgebied, de functies en de technische details worden beschreven, definitief zijn vastgesteld.

Evaluatie- en vervalbepaling

De Commissie moet elk instrument waarop deze mededeling betrekking heeft, evalueren. Dit moet gebeuren in het licht van het gehele bestaande instrumentarium op het gebied van informatiebeheer. Dat moet een betrouwbaar beeld opleveren van de plaats van elk instrument in het grotere geheel van het interneveiligheids- en migratiebeheer. Toekomstige voorstellen moeten, waar nodig, bepalingen bevatten inzake een verplicht jaarlijks verslag, periodieke en

[91] De algemene beginselen en minimumnormen voor raadpleging van de betrokken partijen zijn geformuleerd in COM(2002)704 van 11.12.2002.

ad-hoc-evaluaties, alsmede een vervalbepaling. Bestaande instrumenten worden alleen gehandhaafd als zij aan het legitieme doel waarvoor zij zijn ontworpen, blijven beantwoorden. In bijlage II wordt een overzicht geschetst van de evaluatiedata en –mechanismen van elk instrument dat in deze mededeling wordt behandeld.

5. EEN BLIK VOORUIT

In deze mededeling wordt voor het eerst een helder en volledig overzicht gegeven van alle EU-maatregelen op het gebied van de verzameling, de opslag en de grensoverschrijdende uitwisseling van persoonsgegevens met het oog op rechtshandhaving en migratiebeheer die al zijn ingevoerd, die nu worden ingevoerd of waarover wordt gesproken.

De mededeling biedt burgers inzicht in welke gegevens er over hen worden verzameld, opgeslagen of uitgewisseld, voor welk doel dat gebeurt en door wie. Zij kan tevens als referentiekader dienen voor betrokkenen die zich willen mengen in de discussie over de toekomstige koers van het EU-beleid op dit gebied. Tegelijkertijd vormt de mededeling een eerste antwoord op het verzoek van de Europese Raad om EU-instrumenten voor informatiebeheer te ontwikkelen overeenkomstig de strategie voor het beheer van rechtshandhavingsinformatie[92] en om na te denken over de vraag of er een Europees model voor informatie-uitwisseling moet komen[93].

De Commissie is voornemens als follow-up van deze mededeling in 2012 te komen met een mededeling over een Europees model voor informatie-uitwisseling[94]. Daarom is de Commissie in januari 2010 begonnen met "information mapping" over de rechtsgrondslagen en de praktische werking van de uitwisseling van criminele inlichtingen en gegevens tussen de lidstaten; de Commissie wil de resultaten hiervan in 2011 aan de Raad en het Europees Parlement voorleggen[95].

Ten slotte schetst deze mededeling voor het eerst de visie van de Commissie op de beginselen die zij wil volgen bij de toekomstige ontwikkeling van instrumenten voor het verzamelen, opslaan of uitwisselen van gegevens. Deze beginselen zullen ook worden gevolgd bij het evalueren van de bestaande instrumenten. Naar verwachting zal een dergelijke principiële aanpak van beleidsontwikkeling en –evaluatie de samenhang en de effectiviteit van de bestaande en toekomstige instrumenten vergroten op een wijze die de grondrechten van de burgers ten volle eerbiedigt.

---

92 Conclusies van de Raad over een strategie voor het beheer van rechtshandhavingsinformatie voor interne veiligheid in de EU; Raad Justitie en Binnenlandse Zaken, 30.11.2009.

93 Het programma van Stockholm - Een open en veilig Europa ten dienste en ter bescherming van de burger, Raadsdocument 5731/10 van 3.3.2010, punt 4.2.2.

94 Dit staat in het actieplan ter uitvoering van het programma van Stockholm (COM(2010)171 van 20.4.2010).

95 Deze "information mapping" vindt plaats in nauwe samenwerking met een information mapping projectteam dat bestaat uit vertegenwoordigers van de EU- en de EVA-lidstaten, Europol, Eurojust, Frontex en de Europese Toezichthouder voor gegevensbescherming.

BIJLAGE I

De onderstaande gegevens en voorbeelden illustreren de praktische werking van de momenteel toegepaste maatregelen voor informatiebeheer.

Schengeninformatiesysteem (SIS)

Totaal aantal SIS-signaleringen in de centrale SIS-database (C.SIS)[96]			
Signaleringscategorie	**2007**	**2008**	**2009**
Bankbiljetten	177 327	168 982	134 255
Blanco documenten	390 306	360 349	341 675
Vuurwapens	314 897	332 028	348 353
Afgegeven documenten	17 876 227	22 216 158	25 685 572
Voertuigen	3 012 856	3 618 199	3 889 098
Gezochte personen (aliassen)	299 473	296 815	290 452
Gezochte personen (eigenlijke naam)	859 300	927 318	929 546
waarvan:			
personen gezocht met het oog op aanhouding voor uitlevering	19 119	24 560	28 666
onderdanen van derde landen voor wie een inreisverbod geldt	696 419	746 994	736 868
vermiste meerderjarigen	24 594	23 931	26 707
vermiste minderjarigen	22 907	24 628	25 612
getuigen of personen die zijn gedagvaard	64 684	72 958	78 869
personen onder uitzonderlijk toezicht vanwege een bedreiging voor de openbare veiligheid	31 568	34 149	32 571
personen onder uitzonderlijk toezicht vanwege een bedreiging voor de nationale veiligheid	9	98	253
Totaal	**22 933 370**	**27 919 849**	**31 618 951**

[96] Document 6162/10 van de Raad, 5.2.2010; document 5764/09 van de Raad, 28.1.2009; document 5441/08 van de Raad, 30.1.2008.

Eurodac: asielzoekers die een nieuwe asielaanvraag indienen in dezelfde lidstaat of in andere lidstaten (2008)

Lidstaten die vingerafdrukken inzenden ter vergelijking – treffers uit de lidstaten (kolommen) waar een eerdere asielaanvraag is ingediend	Lidstaat waar de eerste asielaanvraag is ingediend[97]																														Totaal 2e aanvragen	
	AT	BE	BG	CH	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IS	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	UK	**Treffers zelfde land**	**Treffers totaal**
AT	1 725	74	2	0	1	87	274	5	2	31	12	25	115	212	5	0	134	3	14	0	9	52	49	1 371	1	42	111	17	260	61	**1 725**	**4 694**
BE	180	5 450	4	0	3	38	408	17	0	41	17	28	378	67	28	0	69	3	37	0	2	180	73	625	6	3	192	17	58	205	**5 450**	**8 129**
BG	5	2	116	0	1	1	5	1	0	7	0	0	0	1	0	0	1	0	2	0	0	1	3	0	0	6	8	0	0	4	**116**	**164**
CH	32	52	1	4	3	5	35	0	0	17	17	8	39	19	1	0	355	0	1	0	13	15	37	3	1	0	41	4	4	25	**4**	**732**
CY	1	0	0	0	68	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	**68**	**73**
CZ	55	12	0	0	0	637	48	4	0	0	3	4	13	0	1	0	8	2	1	0	0	7	6	17	1	0	13	0	1	6	**637**	**839**
DE	260	268	12	0	4	79	1 852	42	0	174	39	56	256	106	9	2	200	5	26	2	5	174	137	149	4	43	567	30	89	128	**1 852**	**4 718**
DK	44	43	3	0	0	13	126	119	0	27	13	44	36	13	4	0	47	0	7	0	0	30	225	55	2	4	436	2	7	41	**119**	**1 341**
EE	0	0	0	0	0	0	1	1	0	0	0	8	0	0	0	0	0	0	0	0	0	0	1	0	0	0	3	0	0	9	**0**	**23**
EL	66	88	27	0	12	9	131	10	0	766	8	8	35	3	9	0	48	0	1	0	0	33	24	3	0	13	141	0	8	316	**766**	**1 759**
ES	16	18	2	0	1	3	37	1	0	11	108	0	29	4	5	0	35	0	0	0	0	9	9	4	6	0	21	5	1	16	**108**	**341**
FI	37	44	1	0	1	10	115	25	0	48	5	229	14	30	10	1	194	0	3	0	90	49	107	44	2	4	362	3	3	81	**229**	**1512**
FR	365	339	0	0	8	97	502	29	0	92	78	31	860	161	8	0	336	11	26	1	29	106	74	1 739	8	9	286	37	75	190	**860**	**5 497**
HU	297	53	4	0	1	3	169	4	0	2	3	19	70	791	1	0	27	1	10	0	0	28	32	0	0	76	79	19	14	14	**791**	**1 717**
IE	20	21	0	0	4	2	24	1	0	9	8	0	23	4	309	0	35	0	4	0	4	16	7	0	0	0	22	2	2	187	**309**	**704**
IS	4	3	0	0	0	0	3	0	0	3	1	1	6	2	1	0	3	0	1	0	1	3	10	1	0	0	11	1	0	3	**0**	**58**
IT	390	111	5	0	6	33	349	11	0	270	47	27	192	60	23	5	3 290	0	11	0	58	78	116	9	2	6	201	59	224	680	**3 290**	**6 263**
LT	3	1	0	0	1	3	0	0	0	0	1	0	1	0	0	0	0	5	0	0	0	0	4	14	0	0	5	0	2	0	**5**	**40**
LU	7	21	4	0	0	0	12	2	0	0	0	1	9	6	0	1	8	0	2	0	1	6	4	0	0	0	10	3	1	3	**2**	**101**
LV	3	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	5	0	0	0	0	0	0	0	0	1	0	2	0	**0**	**15**
MT	1	0	0	0	0	0	0	0	0	0	0	5	1	0	0	0	6	0	0	0	16	0	1	0	0	0	1	1	0	0	**16**	**32**
NL	109	223	16	0	1	27	198	21	0	113	16	29	109	33	7	1	226	0	14	0	58	1 240	95	16	8	9	289	8	22	129	**1 240**	**3 017**
NO	84	103	6	0	2	13	256	76	0	199	55	57	78	23	8	0	524	8	13	1	83	86	276	164	1	9	826	10	21	96	**276**	**3 078**
PL	188	65	0	0	0	30	68	15	0	0	2	4	75	1	1	0	0	3	3	0	0	7	27	1 208	1	1	43	1	13	4	**1 208**	**1 760**
PT	1	10	0	0	0	0	4	1	0	0	11	0	9	0	0	0	2	0	2	0	0	2	2	0	3	0	2	0	1	2	**3**	**52**
RO	43	2	5	0	1	9	33	0	0	3	0	5	14	11	0	0	0	0	1	0	0	9	1	1	0	64	17	0	4	4	**64**	**227**
SE	243	133	30	0	4	36	516	173	0	143	29	143	145	80	16	3	276	0	16	0	130	98	430	147	5	13	1 914	11	26	122	**1 914**	**4 882**
SI	14	4	0	0	0	1	10	1	0	1	1	2	15	6	0	0	5	0	1	0	0	2	3	0	0	0	5	45	3	2	**45**	**121**
SK	105	4	0	0	0	7	33	0	1	0	0	1	2	12	0	0	3	0	0	1	0	4	4	4	0	0	9	2	195	6	**195**	**393**
UK	109	153	7	0	3	12	276	30	0	108	6	38	209	25	217	2	768	0	8	0	43	128	76	7	4	11	174	6	46	3,141	**3 141**	**5 607**
Totaal 1e aanvragen	**4 407**	**7 298**	**245**	**4**	**125**	**1 155**	**5 487**	**589**	**4**	**2 067**	**480**	**773**	**2 734**	**1 670**	**663**	**15**	**6 600**	**46**	**204**	**5**	**542**	**2 363**	**1 833**	**5 581**	**55**	**313**	**5 791**	**283**	**1 082**	**5 475**	**24 433**	**57 889**

[97] COM (2009) 494 van 25.9.2009. Met "treffers zelfde land" wordt gedoeld op een tweede asielaanvraag die in dezelfde lidstaat wordt ingediend als de eerste aanvraag.

Systeem voor Advance Passenger Information (API)

Gebruik van Advance Passenger Information door het Verenigd Koninkrijk ter verbetering van de grensbewaking en ter bestrijding van illegale migratie[98]	
Aantal maatregelen in 2009	
Negatieve voorgeschiedenis (toelating geweigerd)	379
Verloren, gestolen of ingetrokken paspoorten (reisdocument in beslag genomen)	56

[98] De informatie is door het UK Border Agency aan de Commissie verstrekt ten behoeve van deze mededeling.

Douane-informatiesysteem (DIS)

In 2009 in de DIS-database ingevoerde records[99]	
Actie	**DIS (op basis van DIS-overeenkomst)**
Records aangemaakt	2 007
Records actief	274
Records opgevraagd	11 920
Records gewist	1 355

[99] Informatie verstrekt door de Commissie.

Zweeds initiatief

Voorbeelden van het gebruik van het Zweeds initiatief voor het onderzoek van strafbare feiten[100]	
Doodslag	In 2009 vond in de hoofdstad van een lidstaat een poging tot doodslag plaats. De politie nam een biologisch monster af van een glas waaruit de verdachte had gedronken. Met het uit dit monster verkregen DNA stelden forensische wetenschappers een DNA-profiel op. Vergelijking van dit profiel met andere referentieprofielen in de nationale DNA-database leverde geen resultaat op. De onderzoekende politiedienst diende daarom via het Prümcontactpunt een verzoek in om het profiel te vergelijken met de DNA-referentieprofielen in andere lidstaten die dergelijke gegevens mochten uitwisselen op grond van het Prümbesluit of de Prümovereenkomst. Deze grensoverschrijdende vergelijking leidde tot een treffer. De onderzoekende politiedienst verzocht op grond van het Zweedse initiatief om nadere gegevens betreffende de verdachte. Het nationale contactpunt kreeg binnen 36 uur antwoord uit een aantal andere lidstaten, aan de hand waarvan de politie de verdachte kon identificeren.
Verkrachting	In 2003 werd een vrouw door een onbekende verkracht. De politie nam monsters bij het slachtoffer, maar het daaruit verkregen DNA-profiel stemde overeen met geen van de referentieprofielen in de nationale DNA-database. De politie diende via het Prümcontactpunt een verzoek in om het profiel te vergelijken met de DNA-referentieprofielen in andere lidstaten die dergelijke gegevens mochten uitwisselen op grond van het Prümbesluit of de Prümovereenkomst. Dit leverde een treffer op. De onderzoekende politiedienst verzocht op grond van het Zweedse initiatief om nadere gegevens betreffende de verdachte. Het nationale contactpunt kreeg binnen acht uur antwoord, aan de hand waarvan de politie de verdachte kon identificeren.

[100] Deze informatie is door de politie van een lidstaat aan de Commissie verstrekt ten behoeve van deze mededeling.

Treffers voor Duitsland bij de grensoverschrijdende vergelijking van DNA-profielen, ingedeeld volgens soort delict[101]					
Treffers volgens soort delict	**Oostenrijk**	**Spanje**	**Luxemburg**	**Nederland**	**Slovenië**
Delicten tegen de openbare veiligheid	32	4	0	5	2
Delicten tegen de persoonlijke vrijheid	9	3	5	2	0
Seksuele delicten	40	22	0	31	4
Delicten tegen personen	49	24	0	15	2
Overige delicten	3 005	712	18	1 105	71

[101] Antwoord van de Duitse overheid op een parlementaire vraag van Ulla Jelpke, Inge Höger en Jan Korte (referentienummer 16/14120), Bundestag, 16e zittingsperiode, referentienummer 16/14150, 22.10.2009. Deze cijfers betreffen de periode vanaf de datum waarop de gegevensuitwisseling van een lidstaat met Duitsland begint tot en met 30 september 2009.

Voorbeelden van ernstige misdrijven die zijn ontdekt dankzij gegevensbewaring[102]	
Moord	De politie van een lidstaat kon de daders van een racistische moord op zes personen opsporen. De daders trachtten te ontkomen door hun SIM-kaart te verwisselen, maar dankzij de gesprekkenlijst en de identificatiecode voor mobiele apparatuur konden zij worden aangehouden.
Doodslag	De politie kon bewijzen dat twee verdachten betrokken waren bij een geval van doodslag door de verkeersgegevens van de mobiele telefoon van het slachtoffer te analyseren. Aan de hand hiervan konden rechercheurs de route reconstrueren die het slachtoffer en de twee verdachten samen hadden afgelegd.
Inbraak	De autoriteiten spoorden de dader van 17 inbraken op door de verkeersgegevens van zijn anonieme prepaid-SIM-kaart te analyseren. Door de identiteit van zijn vriendin vast te stellen, kon ook de dader worden opgespoord.
Fraude	Rechercheurs losten een oplichtingszaak op waarbij een bende op internet adverteerde met dure auto's die contant moesten worden betaald. Kopers die hun auto kwamen ophalen, werden door de bende systematisch beroofd. Aan de hand van een IP-adres kon de politie de abonnee opsporen en de daders arresteren.

[102] Deze anonieme voorbeelden zijn ontleend aan de antwoorden van lidstaten op een vragenlijst van de Commissie uit 2009 betreffende de omzetting van Richtlijn 2006/24/EG (richtlijn gegevensbewaring).

Samenwerking tussen financiële inlichtingeneenheden

Aantal informatieverzoeken van nationale financiële inlichtingeneenheden via FIU.net[103]		
Jaar	**Informatieverzoeken**	**Actieve gebruikers**
2007	3 133	12 lidstaten
2008	3 084	13 lidstaten
2009	3 520	18 lidstaten

[103] De informatie is door het FIU.net-bureau aan de Commissie verstrekt ten behoeve van deze mededeling.

Samenwerking tussen bureaus voor de ontneming van vermogensbestanddelen

Verzoeken tot opsporing van vermogensbestanddelen die door lidstaten zijn ingediend en zijn behandeld door Europol[104]				
Jaar	**2004**	**2005**	**2006**	**2007**
Aantal verzoeken	5	57	53	133
waarvan:				
fraude				29
witwassen				26
drugs				25
andere strafbare feiten				18
drugs en witwassen				19
fraude en witwassen				7
andere combinaties van strafbare feiten				9

Door Eurojust behandelde zaken waarbij vermogensbestanddelen verbeurd zijn verklaard (2006–2007)[105]			
Soort zaak		**Procedure ingeleid door**	
milieudelicten	1	Duitsland	27%
deelneming aan een criminele organisatie	5	Nederland	21%
drugshandel	15	Verenigd Koninkrijk	15%
belastingfraude	8	Finland	13%
fraude	8	Frankrijk	8%
btw-fraude	1	Spanje	6%
witwassen	9	Portugal	4%
corruptie	1	Zweden	2%
vermogensdelicten	2	Denemarken	2%
wapensmokkel	1	Letland	2%
namaak en piraterij	2		
voorschotfraude	2		
vervalsing van administratieve documenten	1		
handel in gestolen voertuigen	1		
terrorisme	1		
vervalsing	2		
mensenhandel	1		

104 *Assessing the effectiveness of EU Member States' practices in the identification, tracing, freezing and confiscation of criminal assets – Final Report* (voor DG JLS van de Europese Commissie opgesteld door Matrix Insight, 6.2009).

105 Ibid.

Signaleringsplatforms voor cybercriminaliteit

Voorbeelden van onderzoek naar cybercriminaliteit door het Franse signaleringsplatform voor cybercriminaliteit *Pharos*[106]	
Kinderpornografie	Een internetgebruiker maakte Pharos opmerkzaam op het bestaan van een blog met foto's en cartoonachtige afbeeldingen van seksueel misbruik van kinderen. De auteur van het blog, die op één afbeelding ongekleed was afgebeeld, maakte zich op zijn blog ook schuldig aan "grooming" van kinderen. De rechercheurs identificeerden een wiskundeleraar als de hoofdverdachte. Een huiszoeking leverde 49 kinderpornografische video's op. Uit het onderzoek bleek ook dat hij van plan was thuis bijles te gaan geven. De verdachte werd veroordeeld tot een voorwaardelijke gevangenisstraf.
Kindermisbruik	De Franse politie kreeg een tip over een persoon die op het internet geld bood voor seks met kinderen. Een Pharos-rechercheur die zich als minderjarige voordeed, legde contact met de verdachte, die hem geld bood in ruil voor seks. Aan de hand van de daaropvolgende chatsessie kon Pharos het IP-adres van de verdachte vaststellen, waarna hij afkomstig bleek uit een stad die bekend stond om het veelvuldig voorkomen van seksueel kindermisbruik. De verdachte werd daarop veroordeeld tot een voorwaardelijke gevangenisstraf.

[106] Pharos staat voor: plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements.

Europol

Voorbeelden van de bijdrage van Europol aan de bestrijding van ernstige grensoverschrijdende criminaliteit[107]	
Operatie Andromeda	In december 2009 verleende Europol medewerking aan het opzetten van een grote grensoverschrijdende politieoperatie tegen een netwerk voor drugshandel met contacten in 42 landen. Het netwerk had zijn basis in België en Noorwegen en smokkelde drugs uit Peru, via Nederland, naar België, het Verenigd Koninkrijk, Italië en andere lidstaten. De samenwerking tussen de politiekorpsen werd gecoördineerd door Europol en de justitiële samenwerking door Eurojust. De deelnemende autoriteiten zetten een mobiel kantoor op in Pisa en Europol een actiecentrum in Den Haag. Europol zorgde voor kruisverwijzingen tussen de verdachten en maakte een overzicht van het criminele netwerk.
Deelnemers	Italië, Nederland, Duitsland, België, het Verenigd Koninkrijk, Litouwen, Noorwegen en Eurojust.
Resultaten	De deelnemende politiekorpsen namen 49 kg cocaïne, 10 kg heroïne, 6 000 ecstasypillen, twee vuurwapens, vijf valse identiteitsdocumenten en 43 000 euro in contanten in beslag. 15 personen werden gearresteerd.
Operatie Typhon	Van april 2008 tot februari 2010 verleende Europol analytische steun aan politiekorpsen uit twintig landen die aan Operatie Typhon deelnamen. Bij deze grote operatie tegen een netwerk van pedofielen die via een Oostenrijkse website kinderpornografie uitwisselden, zorgde Europol voor technische ondersteuning en analyse van criminele inlichtingen op basis van de uit Oostenrijk ontvangen beelden. Europol beoordeelde de betrouwbaarheid van de gegevens en bracht deze in kaart. Op basis daarvan stelde Europol zijn eigen inlichtingenmateriaal op. Door kruisverbanden te leggen met de informatie in het onderzoeksdossier produceerde Europol 30 inlichtingenrapporten, naar aanleiding waarvan in diverse landen onderzoek werd verricht.
Deelnemers	België, Bulgarije, Canada, Denemarken, Duitsland, Frankrijk, Hongarije, Italië, Litouwen, Luxemburg, Malta, Nederland, Oostenrijk, Polen, Roemenië, Slovenië, Slowakije, Spanje, het Verenigd Koninkrijk en Zwitserland.
Resultaten	De deelnemende korpsen identificeerden 286 verdachten, waarvan er 118 werden aangehouden. Vijf misbruikslachtoffers in vier landen werden gered.

[107] De informatie is door Europol aan de Commissie verstrekt ten behoeve van deze mededeling. Nadere informatie over Operatie Andromeda is te vinden op http://www.eurojust.europa.eu/.

Voorbeelden van de coördinatie door Eurojust van grote grensoverschrijdende justitiële operaties tegen ernstige criminaliteit[108]	
Mensenhandel en financiering van terrorisme	In mei 2009 coördineerde Eurojust een grensoverschrijdende operatie die tot de arrestatie leidde van vijf leden van een crimineel netwerk dat actief is in Afghanistan, Pakistan, Roemenië, Albanië en Italië. De groep voorzag Afghanen en Pakistani's van valse documenten en smokkelde hen via Iran, Turkije en Griekenland naar Italië. Na aankomst in Italië werden de migranten naar Duitsland, Zweden, België, het Verenigd Koninkrijk en Noorwegen gestuurd. De opbrengsten waren bestemd voor de financiering van terrorisme.
Fraude met bankpassen	Door de coördinatie van grensoverschrijdende politiële en justitiële samenwerking droegen Europol en Eurojust bij aan de ontmanteling van een netwerk dat zich met bankpasfraude bezighield in Ierland, Italië, Nederland, België en Roemenië. Dit netwerk had de identificatiegegevens van zo'n 15 000 betaalkaarten gestolen en daarmee een verlies van 6,5 miljoen euro veroorzaakt. Ter voorbereiding van de operatie vergemakkelijkten Belgische, Ierse, Italiaanse, Nederlandse en Roemeense magistraten de afgifte van Europees aanhoudingsbevelen en de afhandeling van aftapverzoeken tegen verdachten. De operatie leidde in juli 2009 tot 24 arrestaties.
Mensen- en drugshandel	Na een door Eurojust georganiseerde coördinatiebijeenkomst in maart 2009 arresteerden de Italiaanse, Nederlandse en Colombiaanse autoriteiten 62 verdachten van mensen- en drugshandel. Het netwerk smokkelde kwetsbare vrouwen van Nigeria naar Nederland en dwong hen tot prostitutie in Italië, Frankrijk en Spanje. Met de opbrengsten van de prostitutie financierde het netwerk de aankoop van cocaïne in Colombia, bestemd voor consumptie in de EU.

[108] Deze voorbeelden zijn ontleend aan http://www.eurojust.europa.eu/.

Passenger Name Records (PNR)

Gevallen waarbij PNR-analyse informatie opleverde over ernstige grensoverschrijdende criminaliteit[109]	
Kinderhandel	Uit PNR-analyse bleek dat drie onbegeleide kinderen vanuit een EU-lidstaat naar een derde land reisden, terwijl onduidelijk was wie hen daar zou afhalen. De autoriteiten van het derde land werden na het vertrek door de politie van de lidstaat gewaarschuwd, en arresteerden de persoon die de kinderen kwam ophalen: een in de lidstaat geregistreerde seksuele delinquent.
Mensenhandel	Uit PNR-analyse bleek dat een groep mensenhandelaars altijd via dezelfde route reisde. Zij gebruikten valse documenten om op een vlucht binnen de EU in te checken, maar checkten ook met echte documenten in op een vlucht naar een derde land. Vanuit de vertrekhal stapten zij vervolgens in op de vlucht binnen de EU.
Fraude met kredietkaarten	Een aantal gezinnen reisde naar een lidstaat met tickets die met gestolen kredietkaarten waren aangeschaft. Uit onderzoek bleek dat een misdaadorganisatie met deze kaarten tickets aanschafte, die vervolgens in belwinkels werden verkocht. Dankzij de PNR-gegevens kon het verband worden gelegd tussen de reizigers en de kredietkaarten en de verkopers.
Drugshandel	De politie van een lidstaat beschikte over informatie dat een persoon drugs smokkelde vanuit een derde land, maar grenswachten troffen bij zijn aankomst nooit iets aan. Uit de PNR-gegevens bleek dat hij altijd samen reisde met een medeplichtige. Onderzoek wees uit dat deze medeplichtige grote hoeveelheden drugs bij zich had.

[109] De voorbeelden zijn geanonimiseerd om de bron van de informatie te beschermen.

Programma voor het traceren van terrorismefinanciering (Terrorist Finance Tracking Program, TFTP)

Voorbeelden waarbij het TFTP informatie opleverde over terreurplannen[110]	
Verijdelde terreuraanslag Barcelona 2008	In januari 2008 werden in Barcelona tien verdachten gearresteerd in verband met een verijdelde aanslag op het openbaarvervoersnet aldaar. Aan de hand van TFTP-gegevens werd vastgesteld dat de verdachten banden hadden met Azië, Afrika en Noord-Amerika.
Mislukte vloeistof-bomaanslag op trans-Atlantische vlucht 2006	Aan de hand van TFTP-informatie konden verdachten worden onderzocht en veroordeeld die van plan waren in augustus 2006 tien trans-Atlantische vluchten vanuit het Verenigd Koninkrijk naar de VS en Canada op te blazen.
Bomaanslagen Londen 2005	Dankzij TFTP-gegevens konden de rechercheurs nieuwe sporen ontdekken, de identiteit van de verdachten bevestigen en banden aan het licht brengen tussen de daders van de aanslagen.
Bomaanslagen Madrid 2004	Aan een aantal EU-lidstaten werden TFTP-gegevens verstrekt ter ondersteuning van onderzoeken die na de aanslagen werden gestart.

[110] Tweede verslag over de verwerking van persoonsgegevens uit de EU door het United State Treasury Department ten behoeve van terrorismebestrijding. Rechter Jean-Louis Brugière, januari 2010.

BIJLAGE II

Overzichtstabel van instrumenten die in werking, in uitvoering of gepland zijn

Instrument	Achter-grond	Doel	Structuur	Betrokken persoonsgegevens	Toegang tot gegevens	Gegevens-bescherming	Gegevens-bewaring	Stand van uitvoering	Toetsing
Schengen-informatie-systeem (SIS)	Geïnitieerd door lidstaten	Handhaving van de openbare veiligheid, waaronder de nationale veiligheid, in het Schengengebied en vergemakkelijking van het personenverkeer met behulp van de informatie die via dit systeem wordt doorgegeven.	Gecentraliseerd: N.SIS (nationale delen) via interface verbonden met C.SIS (centraal deel).	Namen en aliassen, fysieke kenmerken, geboorteplaats en -datum, nationaliteit; of betrokkene gewapend en/of gewelddadig is. SIS-signaleringen kunnen betrekking hebben op diverse categorieën personen.	Politie, grenspolitie, douane en gerechtelijke autoriteiten hebben toegang tot alle gegevens. Immigratieautoriteiten en consulaire autoriteiten krijgen toegang tot de lijst van personen met een inreisverbod en signaleringen betreffende verdwenen of gestolen documenten. Europol en Eurojust hebben toegang tot sommige gegevens.	Verdrag 108 Raad van Europa en Politieaanbeveling R(87) 15 Raad van Europa.	In SIS ingevoerde persoonsgegevens mogen niet langer worden bewaard dan nodig is voor het doel waarvoor ze zijn verstrekt, en in ieder geval niet langer dan drie jaar. Gegevens over personen die onder uitzonderlijk toezicht worden geplaatst omdat zij een bedreiging vormen voor de openbare of de nationale veiligheid moeten na een jaar worden verwijderd.	SIS is volledig in gebruik genomen in 22 lidstaten en in Zwitserland, Noorwegen en IJsland. Het Verenigd Koninkrijk en Ierland nemen deel aan SIS, behalve voor signaleringen van onderdanen van derde landen met een inreisverbod. Bulgarije, Roemenië en Liechtenstein zullen SIS naar verwachting vanaf 2011 invoeren.	De ondertekenaars kunnen wijzigingen van de Schengenuitvoeringsovereenkomst voorstellen. De gewijzigde tekst moet unaniem worden goedgekeurd en door de parlementen worden geratificeerd.

Overzichtstabel van instrumenten die in werking, in uitvoering of gepland zijn

Instrument	Achtergrond	Doel	Structuur	Betrokken persoonsgegevens	Toegang tot gegevens	Gegevensbescherming	Gegevensbewaring	Stand van uitvoering	Toetsing
Schengen-informatiesysteem II (SIS II)	Geïnitieerd door de Commissie.	Garanderen van een hoog veiligheidsniveau in de ruimte van vrijheid, veiligheid en recht; vergemakkelijking van het personenverkeer met behulp van de informatie die via dit systeem wordt doorgegeven.	Gecentraliseerd: N.SIS II (nationale delen) via interface verbonden met CS.SIS (centraal deel). SIS II werkt via het beveiligde s-TESTA-netwerk.	De gegevenscategorieën van SIS, plus vingerafdrukken, foto's, kopieën van het Europees aanhoudingsbevel, signaleringen in verband met identiteitsmisbruik en links tussen signaleringen. SIS II-signaleringen kunnen betrekking hebben op diverse categorieën personen.	Politie, grenspolitie, douane en gerechtelijke autoriteiten krijgen toegang tot alle gegevens. Immigratieautoriteiten en consulaire autoriteiten krijgen toegang tot de lijst van personen met een inreisverbod en signaleringen betreffende verdwenen of gestolen documenten. Europol en Eurojust krijgen toegang tot sommige gegevens.	Specifieke voorschriften in de basisbesluiten voor SIS II en in Richtlijn 95/46/EG, Verordening nr. 45/2001, Kaderbesluit 2008/977/JBZ van de Raad, Verdrag nr. 108 Raad van Europa en politieaanbeveling R(87) 15 Raad van Europa.	In SIS ingevoerde persoonsgegevens mogen niet langer worden bewaard dan nodig is voor het doel waarvoor ze zijn verstrekt, en in ieder geval niet langer dan drie jaar. Gegevens over personen die onder uitzonderlijk toezicht worden geplaatst omdat zij een bedreiging vormen voor de openbare of de nationale veiligheid moeten na een jaar worden verwijderd.	SIS II is in uitvoering. Na inbedrijfstelling zal het gebruikt worden in EU-27, Zwitserland, Liechtenstein, Noorwegen en IJsland. Het Verenigd Koninkrijk en Ierland zullen deelnemen aan SIS II, behalve voor signaleringen van onderdanen van derde landen met een inreisverbod.	De Commissie zendt tweejaarlijkse voortgangsverslagen aan het Europees Parlement en de Raad over de ontwikkeling van SIS II en de mogelijke migratie vanuit SIS.
EURODAC	Geïnitieerd door de Commissie.	Helpt de lidstaten vast te stellen welk land een asielverzoek moet beoordelen.	Gecentraliseerd, bestaat uit nationale toegangspunten die via een interface verbonden zijn met de centrale eenheid van Eurodac. Eurodac werkt via het s-TESTA-netwerk.	Vingerafdrukken, geslacht, plaats en datum van de asielaanvraag, referentienummer dat door de lidstaat van oorsprong wordt gebruikt en datum waarop de vingerafdrukken zijn genomen, verzonden en in het systeem ingevoerd.	De lidstaten moeten aangeven welke autoriteiten toegang hebben tot de gegevens; meestal zijn dat asiel- en migratieautoriteiten, grenswacht en politie.	Richtlijn 95/46/EG	Tien jaar voor vingerafdrukken van asielzoekers en twee jaar voor onderdanen van derde landen die zijn aangehouden in verband met illegale overschrijding van een buitengrens.	De Eurodac-verordening is van kracht in elke lidstaat en in Noorwegen, IJsland en Zwitserland. Een overeenkomst betreffende de aansluiting van Liechtenstein is gereed om te worden gesloten.	De Commissie moet jaarlijks bij het Europees Parlement en de Raad een verslag indienen over de werking van de centrale eenheid van Eurodac.

Overzichtstabel van instrumenten die in werking, in uitvoering of gepland zijn

Instrument	Achter-grond	Doel	Structuur	Betrokken persoonsgegevens	Toegang tot gegevens	Gegevens-bescherming	Gegevens-bewaring	Stand van uitvoering	Toetsing
Visum-informatie-systeem (VIS)	Geïnitieerd door de Commissie.	Helpt bij de invoering van een gemeenschappelijk visumbeleid en het voorkomen van bedreigingen van de interne veiligheid.	Gecentraliseerd, bestaat uit nationale delen die via een interface verbonden zijn met de centrale eenheid. Het VIS werkt via het s-TESTA-netwerk.	Visumaanvragen, vingerafdrukken, foto's, aanverwante besluiten inzake visa en links tussen aanvragen die met elkaar te maken hebben.	Visum-, asiel-, immigratie- en grensbewakingsautoriteiten krijgen toegang tot alle gegevens. Politie en Europol mogen het VIS raadplegen ter voorkoming en bestrijding van ernstige criminaliteit.	Specifieke voorschriften in de basisbesluiten voor het VIS en in Richtlijn 95/46/EG, Verordening nr. 45/2001, Kaderbesluit 2008/977/JBZ van de Raad, Verdrag nr. 108 Raad van Europa, aanvullend protocol 181 en politieaanbeveling R(87) 15 Raad van Europa.	Vijf jaar.	Het VIS wordt momenteel geïmplementeerd en zal van toepassing zijn in alle lidstaten behalve het Verenigd Koninkrijk en Ierland, plus Zwitserland, Noorwegen en IJsland.	De Commissie moet over de werking van het VIS drie jaar na de ingebruikneming rapporteren aan het EP en de Raad en daarna elke vier jaar.
Systeem voor Advance Passenger Information (API)	Geïnitieerd door Spanje.	Verbetering grensbewaking en bestrijding illegale migratie.	Gedecentraliseerd.	Persoonsgegevens van paspoorten, instappunt en grensdoorlaatpost van binnenkomst in de EU.	Grensbewakings-autoriteiten en (op verzoek) rechtshandhavings-autoriteiten.	Richtlijn 95/46/EG	Gegevens moeten worden vernietigd 24 na aankomst van een vlucht in de EU.	API is van kracht in elke lidstaat, maar wordt slechts door enkele ervan gebruikt.	De Commissie zal het API in 2011 evalueren.
Napels II-overeenkomst	Geïnitieerd door lidstaten	De nationale douanediensten in staat stellen inbreuken op de nationale douanevoorschriften te voorkomen en op te sporen en hen helpen inbreuken op de communautaire en de nationale douanevoorschriften te vervolgen en te bestraffen.	Gedecentraliseerd, werkt via een aantal centrale coördinatie-eenheden.	Alle informatie over een geïdentificeerde of te identificeren persoon.	De centrale coördinatie-eenheden geven gegevens door aan nationale douaneautoriteiten, onderzoeksautoriteiten en gerechtelijke instanties, en, met voorafgaande toestemming van de lidstaat die de gegevens verstrekt, aan andere autoriteiten.	Richtlijn 95/46/EG en Verdrag nr. 108 Raad van Europa. De gegevens moeten in de ontvangende lidstaat ten minste even goed worden beschermd als in de verstrekkende lidstaat.	De gegevens mogen niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor ze werden verstrekt.	Alle lidstaten hebben de Napels II-overeenkomst geratificeerd.	De ondertekenaars kunnen wijzigingen van de Napels II-overeenkomst voorstellen. De gewijzigde tekst moet worden goedgekeurd door de Raad en geratificeerd door de lidstaten.

Overzichtstabel van instrumenten die in werking, in uitvoering of gepland zijn

Instrument	Achter-grond	Doel	Structuur	Betrokken persoonsgegevens	Toegang tot gegevens	Gegevens-bescherming	Gegevens-bewaring	Stand van uitvoering	Toetsing
Douane-informatie-systeem (DIS)	Geïnitieerd door lidstaten	Helpt de bevoegde autoriteiten bij het voorkomen, onderzoeken en vervolgen van ernstige overtredingen van de nationale douanewetgeving.	Gecentraliseerd, toegankelijk via terminals in elke lidstaat en bij de Commissie. DIS en FIDE werken op basis van het AFIS, dat gebruik maakt van het gemeenschappelijk communicatienetwerk, de gemeenschappelijke systeeminterface of de beveiligde internettoegang van de Commissie.	Namen en aliassen, geboortedatum en -plaats, nationaliteit, geslacht, fysieke kenmerken, identiteitsdocumenten, adres, eerder voorgekomen gewelddadigheid, reden voor het opnemen van gegevens in DIS, voorgestelde actie en registratiekenmerken van vervoermiddelen.	Nationale douane-autoriteiten, Europol en Eurojust hebben toegang tot DIS-gegevens.	Specifieke voorschriften in de DIS-overeenkomst en in Richtlijn 95/46/EG, Verordening nr. 45/2001, Verdrag nr. 108 Raad van Europa en politie-aanbeveling R(87) 15 Raad van Europa.	Uit het DIS naar andere systemen voor risicobeheersing of operationele analyse gekopieerde persoonsgegevens mogen slechts bewaard blijven zolang dat nodig is om het doel waarvoor ze werden gekopieerd, te verwezenlijken, en in geen geval langer dan tien jaar.	Van kracht in elke lidstaat.	De Commissie brengt elk jaar in samenwerking met de lidstaten verslag uit aan EP en Raad.
Zweeds initiatief	Geïnitieerd door Zweden.	Stroomlijning van informatie-uitwisseling voor strafrechtelijk onderzoek en inlichtingenoperaties.	Gedecentraliseerd, lidstaten wijzen nationale contactpunten aan voor de behandeling van dringende verzoeken om informatie.	Alle gegevens en strafrechtelijke inlichtingen waarover de rechtshandhavingsautoriteiten beschikken.	Politie, douane en andere instanties die bevoegd zijn tot het onderzoeken van misdrijven (m.u.v. inlichtingendiensten).	Nationale regels voor gegevensbescherming, Verdrag 108 Raad van Europa, aanvullend protocol 181 Raad van Europa en Politie-aanbeveling R(87) 15 Raad van Europa.	Via dit instrument verstrekte informatie mag slechts gebruikt worden voor het doel waarvoor zij is verstrekt, onder specifieke voorwaarden die de verstrekkende lidstaat stelt.	12 van de 31 ondertekenaars (EU- en EVA-staten) hebben nationale wetgeving vastgesteld ter uitvoering van dit instrument; vijf staten gebruiken het formulier voor verzoek om gegevens en twee gebruiken het vaak voor informatie-uitwisseling.	De Commissie zal haar evaluatieverslag in 2010 indienen bij de Raad.

Overzichtstabel van instrumenten die in werking, in uitvoering of gepland zijn									
Instrument	**Achter-grond**	**Doel**	**Structuur**	**Betrokken persoonsgegevens**	**Toegang tot gegevens**	**Gegevens-bescherming**	**Gegevens-bewaring**	**Stand van uitvoering**	**Toetsing**
Prümbesluit	Geïnitieerd door lidstaten.	Verbetering van misdaadpreventie, met name wat terrorisme betreft, en handhaving van de openbare orde.	Gedecentraliseerd, verbonden via het s-TESTA-netwerk. Nationale contact-punten behandelen inkomende en uit-gaande verzoeken om vergelijking van gegevens.	Anonieme DNA-profielen en vinger-afdrukken, voertuig-registratiegegevens en informatie over personen die ver-dacht worden van banden met terroris-ten.	De contactpunten geven verzoeken door; voor de binnenlandse toegang geldt de nationale wet.	Specifieke regels van het Prüm-besluit en Verdrag 108 Raad van Europa, aanvul-lend protocol 181 Raad van Europa en Politieaanbeve-ling R(87) 15 Raad van Europa. Per-sonen kunnen zich tot de nationale gegevensbescher-mingsfunctionaris richten om hun rechten inzake de verwerking van persoonsgegevens af te dwingen.	Persoonsgegevens moeten worden ge-wist wanneer zij niet langer nodig zijn voor het doel waar-voor zij zijn ver-strekt. De maximale bewaringstermijn van de verstrekken-de staat is bindend voor de ontvangen-de staat.	Het Prümbesluit is in uitvoering. Tien lidstaten mogen DNA-gegevens uitwisselen, vijf vingerafdrukken, zeven voertuig-registratiegegevens. Noorwegen en IJs-land treden binnen-kort toe tot dit in-strument.	De Commissie zal haar evaluatieverslag in 2012 indienen bij de Raad.
Richtlijn gegevens-bewaring	Geïnitieerd door lidstaten.	Verbetering van het onderzoeken, opsporen en ver-volgen van ern-stige criminaliteit door bewaring van telecommunicatie-verkeers- en loca-tiegegevens.	Gedecentraliseerd. Het instrument verplicht telecom-municatiedienst-verleners tot het bewaren van gege-vens.	Telefoonnummer, IP-adres en identifi-catiecode van mobie-le apparatuur)	Nationaal wordt bepaald welke in-stanties toegang hebben tot de gege-vens.	Richtlijn 95/46/EG en Richtlijn 2002/58/EG.	6 tot 24 maanden.	Zes lidstaten heb-ben de richtlijn nog niet omgezet. Het constitutionele hof van Duitsland en dat van Roemenië hebben de omzet-tingsmaatregelen ongrondwettig ver-klaard.	De Commissie zal haar evaluatieverslag in 2010 indienen bij EP en Raad.

Overzichtstabel van instrumenten die in werking, in uitvoering of gepland zijn									
Instrument	**Achter-grond**	**Doel**	**Structuur**	**Betrokken persoonsgegevens**	**Toegang tot gegevens**	**Gegevens-bescherming**	**Gegevens-bewaring**	**Stand van uitvoering**	**Toetsing**
Europees Strafregis-terinforma-tiesysteem (ECRIS)	Geïnitieerd door België en voorge-steld door de Commissie.	Verbetering van grensoverschrij-dende informatie-deling betreffende het strafregister van EU-burgers.	Gedecentraliseerd, verbonden via cen-trale instanties die informatie uitwis-selen uit de straf-registers van de lidstaten via het s-Testa-netwerk.	Biografische gege-vens, gegevens be-treffende veroorde-ling, straf en ge-pleegd delict, aan-vullende informatie, zoals vingerafdruk-ken (indien beschik-baar).	Bevoegde justitiële en bestuurlijke instanties.	Specifieke voor-schriften in Kader-besluit 2009/315/JBZ van de Raad, waarin de regels van Besluit 2005/876/JBZ zijn verwerkt, en Ka-derbesluit 2008/977/JBZ van de Raad, Verdrag 108 Raad van Europa en Veror-dening (EG) nr. 45/2001.	De nationale gege-vensbewaringsre-gels zijn van toepas-sing; dit instrument regelt slechts de uit-wisseling.	Ecris is in uitvoering. Negen lidstaten zijn begonnen met elek-tronische informa-tie-uitwisseling.	De Commissie dient twee evaluatie-verslagen in bij het EP en de Raad: in 2011 over Kaderbesluit 2008/675/JBZ en in 2015 over Kaderbesluit 2009/315/JBZ. Vanaf 2016 moet de Com-missie regelmatig verslagen opstellen over de werking van Besluit 2009/316/JBZ van de Raad over Ecris.
Samenwer-king tussen financiële in-lichtingen-eenheden (FIU.net)	Geïnitieerd door Nederland.	Uitwisseling van informatie voor analyse en onderzoek van witwaspraktijken en financiering van terroristen.	Gedecentraliseerd. De inlichtingen-eenheden wisselen gegevens uit via FIU.net, dat via het s-TESTA-netwerk werkt. Waarschijnlijk zal binnenkort gebruik worden gemaakt van de Siena-toepassing van Europol.	Alle gegevens die relevant zijn voor analyse of onderzoek van witwaspraktijken en financiering van terroristische activi-teiten.	Financiële inlich-tingeneenheden (binnen politie-korpsen, justitiële autoriteiten of ad-ministratieve orga-nen die aan finan-ciële autoriteiten rapporteren).	Kaderbesluit 2008/977/JBZ van de Raad, Verdrag 108 Raad van Europa en Politie-aanbeveling R(87) 15 Raad van Europa.	De nationale gege-vensbewaringsre-gels zijn van toepas-sing; dit instrument regelt slechts de uit-wisseling.	20 lidstaten nemen deel aan FIU.net, een online-toepassing voor gegevensdeling die via s-TESTA werkt.	Als onderdeel van haar Actieplan voor financiële diensten evalueert de Com-missie de uitvoering van Richtlijn 2005/60/EG sinds 2009.

Overzichtstabel van instrumenten die in werking, in uitvoering of gepland zijn

Instrument	Achtergrond	Doel	Structuur	Betrokken persoonsgegevens	Toegang tot gegevens	Gegevensbescherming	Gegevensbewaring	Stand van uitvoering	Toetsing
Samenwerking tussen bureaus voor de ontneming van vermogensbestanddelen	Geïnitieerd door lidstaten.	Uitwisseling van informatie die nodig is voor het opsporen en identificeren van opbrengsten van misdrijven.	Gedecentraliseerd. De bureaus wisselen informatie uit via het Zweedse initiatief. Waarschijnlijk zal binnenkort gebruik worden gemaakt van de Siena-toepassing van Europol.	Gegevens over de beoogde vermogensbestanddelen (zoals bankrekeningen, vastgoed en voertuigen), en gegevens over gezochte personen, zoals naam, adres en aandeelhouders- en bedrijfsgegevens.	Bureaus voor de ontneming van vermogensbestanddelen.	Verdrag 108 Raad van Europa, aanvullend protocol 181 en Politieaanbeveling R(87) 15 Raad van Europa.	De nationale gegevensbewaringsregels zijn van toepassing; dit instrument regelt slechts de uitwisseling.	Ruim 20 lidstaten hebben bureaus voor de ontneming van vermogensbestanddelen opgericht. 12 bureaus nemen deel aan een proefproject voor gebruik van Siena voor het uitwisselen van gegevens over de opsporing van vermogensbestanddelen.	De Commissie zal haar evaluatieverslag in 2010 indienen bij de Raad.
Nationale en Europese cybercriminaliteitplatforms	Geïnitieerd door Frankrijk.	Verzamelen, uitwisselen en analyseren van gegevens over internetcriminaliteit.	Gedecentraliseerd, brengt koppeling tot stand tussen nationale signaleringsplatforms en het Europees cybercriminaliteitplatform. Waarschijnlijk zal binnenkort gebruik worden gemaakt van de Siena-toepassing van Europol.	Illegale inhoud of gedragingen die op internet zijn aangetroffen.	De nationale platforms krijgen meldingen van burgers, Het Europees cybercriminaliteitplatform van Europol krijgt verslagen van rechtshandhavingsinstanties over ernstige grensoverschrijdende cybercriminaliteit.	Specifieke voorschriften in het Europolbesluit en Kaderbesluit 2008/977/JBZ van de Raad, Verdrag nr. 108 Raad van Europa, aanvullend protocol 181 en politieaanbeveling R(87) 15 Raad van Europa en Verordening (EG) nr. 45/2001.	De nationale gegevensbewaringsregels zijn van toepassing; dit instrument regelt slechts de uitwisseling.	Bijna alle lidstaten hebben een nationaal signaleringsplatform opgericht. Europol werkt aan het Europees cybercriminaliteitplatform.	Europol zorgt voor de rapportage over cybercriminaliteit en zal in de toekomst verslag uitbrengen over de activiteiten van het Europees cybercriminaliteitplatform in het jaarverslag, dat ter goedkeuring aan de Raad en ter informatie aan het EP wordt voorgelegd.

Overzichtstabel van instrumenten die in werking, in uitvoering of gepland zijn									
Instrument	**Achter-grond**	**Doel**	**Structuur**	**Betrokken persoonsgegevens**	**Toegang tot gegevens**	**Gegevens-bescherming**	**Gegevens-bewaring**	**Stand van uitvoering**	**Toetsing**
Europol	Geïnitieerd door lidstaten.	Bijstand aan lid-staten bij het voorkomen en bestrijden van georganiseerde misdaad, terrorisme en andere vormen van ernstige crimina-liteit waarbij twee of meer lidstaten betrokken zijn.	Europol is een EU-agentschap dat in Den Haag is gevestigd. Het ontwikkelt Siena, een beveiligde netwerktoepassing voor informatie-uitwisseling.	Het Europol-informatiesysteem (EIS) bevat per-soonsgegevens, waaronder biometri-sche kenmerken, ver-oordelingen en gege-vens over banden met georganiseerde criminaliteit, over personen die worden verdacht van strafbare feiten die onder de bevoegdheid van Europol vallen. De analysebestanden be-vatten alle relevante persoonsgegevens.	Nationale Europol-eenheden, verbin-dingsofficieren, personeelsleden van Europol en de directeur hebben toegang tot het EIS. Verbindingsofficie-ren hebben toegang tot de analysebestanden. Persoonsgegevens mogen worden uit-gewisseld met lan-den waarmee Euro-pol een overeen-komst heeft gesloten.	Specifieke voor-schriften in het Europolbesluit en Kaderbesluit 2008/977/JBZ van de Raad, Verdrag nr. 108 Raad van Europa, aanvul-lend protocol 181 en politieaanbeve-ling R(87) 15 Raad van Europa en Verordening (EG) nr. 45/2001.	Analysebestanden mogen maximaal drie jaar worden bewaard; deze termijn kan worden verlengd met nog eens drie jaar.	Europol wordt actief gebruikt door alle lidstaten en derde landen waarmee een operationele over-eenkomst is gesloten. Alle lid-staten voldoen aan de nieuwe rechts-grondslag van Europol.	Een gemeenschappelijk controleorgaan houdt toezicht op de verwerking van persoonsgegevens door Europol en de doorgifte daarvan aan derden. Het brengt regelmatig verslag uit aan het EP en de Raad. Europol legt daarnaast jaarlijks een verslag over zijn activiteiten ter goedkeuring voor aan de Raad en ter informatie aan het EP.

Overzichtstabel van instrumenten die in werking, in uitvoering of gepland zijn									
Instrument	**Achter-grond**	**Doel**	**Structuur**	**Betrokken persoonsgegevens**	**Toegang tot gegevens**	**Gegevens-bescherming**	**Gegevens-bewaring**	**Stand van uitvoering**	**Toetsing**
Eurojust	Geïnitieerd door lidstaten.	Verbetering van de coördinatie van onderzoek en vervolging in de lidstaten en verbetering van de samenwerking tussen de betrokken autoriteiten.	Eurojust is een EU-agentschap dat in Den Haag is gevestigd. Het gebruikt s-TESTA voor de uitwisseling van gegevens.	Persoonsgegevens van verdachten en daders van ernstige misdrijven waarbij twee of meer lidstaten betrokken zijn, waaronder biografische gegevens, contactgegevens, DNA-profielen, vingerafdrukken, foto's en telecommunicatieverkeers- en locatiegegevens .	De 27 nationale leden van Europol, die gegevens mogen doorgeven aan nationale autoriteiten en derde landen, indien de informatieverstrekker daarmee instemt.	Specifieke regels van het Eurojust-besluit en Kaderbesluit 2008/919/JBZ van de Raad, Verdrag 108 Raad van Europa, aanvullend protocol 181 Raad van Europa en Politie-aanbeveling R(87) 15 Raad van Europa.	De informatie moet worden verwijderd zodra het doel waarvoor zij is verstrekt is bereikt, en wanneer een zaak wordt gesloten.	De lidstaten werken momenteel aan de tenuitvoerlegging van de nieuwe rechtsgrondslag van Eurojust.	In juni 2014 moet de Commissie de uitwisseling van gegevens tussen de nationale leden van Eurojust evalueren. In juni 2013 moet Eurojust verslag uitbrengen aan Raad en Commissie over de nationale verlening van toegang tot het case-managementsysteem. Een gemeenschappelijk controleorgaan houdt toezicht op de verwerking van persoonsgegevens door Europol en brengt jaarlijks verslag uit aan de Raad. De voorzitter van het Eurojustcollege dient jaarlijks bij de Raad een verslag in over de activiteiten van Eurojust, dat de Raad doorstuurt naar het EP.

Overzichtstabel van instrumenten die in werking, in uitvoering of gepland zijn									
Instrument	**Achter-grond**	**Doel**	**Structuur**	**Betrokken persoonsgegevens**	**Toegang tot gegevens**	**Gegevens-bescherming**	**Gegevens-bewaring**	**Stand van uitvoering**	**Toetsing**
PNR-overeenkom-sten met VS en Australië; API/PNR-overeen-komst met Canada	Geïnitieerd door de Commissie.	Voorkoming en bestrijding van terrorisme en andere vormen van ernstige grens-overschrijdende criminaliteit	Internationale overeenkomsten.	De overeenkomsten met de VS en Australië bevatten 19 categorieën PNR-gegevens, waaronder biografische gegevens, boekings-gegevens, beta-lingsgegevens en aanvullende gegevens. De overeenkomst met Canada bevat 25 ver-gelijkbare categorieën.	Department of Homeland Security van de VS, Canada Border Services Agency en Australian Customs Service. Deze mogen gegevens doorgeven aan nationale autoriteiten die belast zijn met rechtshandhaving of terrorismebestrijdin g	De voorschriften inzake gegevens-bescherming zijn opgenomen in de internationale overeenkomsten.	VS: 7 jaar actief gebruik en 8 jaar passief gebruik. Australië: 3,5 jaar actief gebruik en 2 jaar passief gebruik. Canada: 72 uur actief gebruik en 3,5 jaar passief gebruik.	De overeenkomsten met VS en Australië zijn voorlopig van toepassing, die met Canada is in werking getreden. De Commissie zal over deze overeenkomsten opnieuw onderhan-delen. Zes EU-lid-staten hebben wetten die het gebruik van PNR-gegevens voor rechtshandhaving toestaan.	Elk van de overeen-komsten voorziet in periodieke evaluatie. De overeenkomsten met Canada en Aus-tralië bevatten ook een beëindigingsclausule.

Overzichtstabel van instrumenten die in werking, in uitvoering of gepland zijn									
Instrument	**Achter-grond**	**Doel**	**Structuur**	**Betrokken persoonsgegevens**	**Toegang tot gegevens**	**Gegevens-bescherming**	**Gegevens-bewaring**	**Stand van uitvoering**	**Toetsing**
TFTP-over-eenkomst tussen EU en VS	Geïnitieerd door de Commissie.	Voorkomen, onderzoeken, opsporen en vervolgen van de financiering van terrorisme.	Internationale overeenkomst.	Gegevens betreffende financieel berichten-verkeer, zoals naam, rekeningnummer, adres en identificatienummer van de opdracht-gever en ontvangers van financiële transacties.	Het VS-ministerie van Financiën mag persoonsgegevens die het uit het fi-nanciële berichten-verkeer heeft geëx-traheerd, doorgeven aan de Amerikaanse instanties voor rechtshandhaving, openbare veiligheid of terrorismebestrij-ding, aan Europol en aan Eurojust. Doorgifte naar derde landen is slechts geoorloofd met toestemming van de lidstaten.	De overeenkomst bevat strikte doel-bindings- en even-redigheids-clausules.	Informatie die uit verstrekte gegevens over financieel berichtenverkeer wordt geëxtraheerd, mag niet langer worden bewaard dan noodzakelijk is voor het specifieke onderzoek of de specifieke vervolging waarvoor ze wordt gebruikt; niet-geëxtraheerde gegevens mogen maximaal vijf jaar worden bewaard.	Het EP heeft op 8 juli 2010 ingestemd met de sluiting van de TFTP-overeenkomst. De Raad moet nu een besluit vaststellen betreffende de slui-ting van de overeenkomst, waarna deze in werking kan treden door middel van een briefwisseling tussen de partijen.	De Commissie moet de overeenkomst zes maanden na de inwerkingtreding evalueren. Het evaluatieverslag wordt bij het EP en de Raad ingediend.