EUROPESE
COMMISSIE

Brussel, 7.12.2012
COM(2012) 735 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

Samenwerking op het gebied van rechtshandhaving in de EU versterken: het Europees model voor informatie-uitwisseling (EIXM)

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

Samenwerking op het gebied van rechtshandhaving in de EU versterken: het Europees model voor informatie-uitwisseling (EIXM)

1. INLEIDING

Om in de EU en het Schengengebied een hoog niveau van veiligheid te waarborgen, moeten criminele netwerken via gezamenlijk Europees optreden worden aangepakt[1]. Dat is nodig om niet alleen ernstige en georganiseerde criminaliteit aan te pakken, zoals mensenhandel of handel in illegale drugs of vuurwapens, maar ook minder ernstige misdrijven die op grote schaal worden gepleegd door mobiele georganiseerde criminele groepen of misdrijven die door individuele daders worden gepleegd over de grenzen van de lidstaten heen.

Informatie-uitwisseling tussen de lidstaten is in dat verband een belangrijk instrument voor rechtshandhavingsinstanties. Daarom werden internationale en bilaterale overeenkomsten aangevuld met EU-instrumenten en -systemen, zoals het Schengeninformatiesysteem en het Europolinformatiesysteem, met ingebouwde waarborgen om de persoonlijke levenssfeer en de persoonsgegevens te beschermen overeenkomstig het Handvest van de grondrechten. In deze mededeling wordt een stand van zaken opgemaakt van de **manier** waarop de daaruit voortvloeiende **grensoverschrijdende informatie-uitwisseling in de EU vandaag werkt** en worden tevens aanbevelingen gedaan ter verbetering daarvan.

De conclusie luidt dat de informatie-uitwisseling in het algemeen goed werkt en om dat te illustreren, worden voorbeelden gegeven van gunstige resultaten. **Derhalve is er op EU-niveau vooralsnog geen behoefte aan nieuwe gegevensbanken of informatie-uitwisselingsinstrumenten op het gebied van rechtshandhaving**. De bestaande EU-instrumenten kunnen en moeten echter beter worden uitgevoerd en de uitwisselingen moeten consistenter worden georganiseerd.

Deze mededeling bevat dan ook aanbevelingen voor de lidstaten **over de wijze waarop de uitvoering van bestaande instrumenten kan worden verbeterd** en **de gebruikte communicatiekanalen kunnen worden gestroomlijnd**. De klemtoon ligt daarbij op de noodzaak om **hoge gegevenskwaliteit, veiligheid en bescherming te waarborgen**. In de mededeling wordt ook uiteengezet hoe de Commissie de lidstaten zal steunen, onder meer met **financiering en opleiding**. Op die manier biedt zij een model met richtsnoeren voor activiteiten van de EU en de lidstaten.

Deze mededeling is ook een reactie op het verzoek aan de Commissie in het *programma van Stockholm* om op basis van een evaluatie van de bestaande instrumenten na te gaan of er een Europees model voor informatie-uitwisseling moet komen. Zij bouwt voort op de mededeling van de Commissie van 2010 waarin een overzicht wordt gegeven van het informatiebeheer op het gebied van vrijheid, veiligheid en recht (hierna „de overzichtsmededeling van 2010" genoemd)[2] en op de EU-strategie voor het beheer van rechtshandhavingsinformatie voor

[1] De EU-interneveiligheidsstrategie in actie, COM(2010) 673.

[2] COM(2010) 385.

interne veiligheid die in 2009[3] is overeengekomen, alsook op maatregelen van de lidstaten, de Commissie en Europol ter uitvoering daarvan (hierna „IMS-maatregelen" genoemd). Voorts is rekening gehouden met een inventaris van informatie-uitwisseling in de EU waarbij nationale en andere deskundigen (Europese toezichthouder voor gegevensbescherming, EU-agentschappen, Interpol) betrokken zijn, een studie over informatie-uitwisseling tussen rechtshandhavingsinstanties[4] en overleg met belanghebbenden, waaronder gegevensbeschermingsinstanties.

2. DE HUIDIGE SITUATIE

Rechtshandhavingsinstanties wisselen informatie uit voor uiteenlopende doelen: voor strafrechtelijke onderzoeken, voor criminaliteitspreventie, voor opsporing van strafbare feiten (bv. met gebruikmaking van criminele-inlichtingenoperaties) en voor het waarborgen van de openbare orde en veiligheid. Wat de omvang van de grensoverschrijdende uitwisseling betreft, blijkt uit de in de bovengenoemde studie van 2010 door nationale instellingen van de lidstaten gegeven antwoorden dat in ongeveer een kwart van hun onderzoeken en criminele-inlichtingenoperaties verzoeken werden gericht aan andere EU- of Schengenstaten.

2.1. Instrumenten

In de overzichtsmededeling van 2010 werden alle EU-instrumenten beschreven die de verzameling, de opslag of de grensoverschrijdende uitwisseling van persoonsgegevens met het oog op rechtshandhaving of migratiebeheer regelen. In deze mededeling gaat het over **instrumenten die worden gebruikt voor de grensoverschrijdende uitwisseling tussen lidstaten**. De lidstaten hebben voorbeelden gegeven van wijzen waarop deze instrumenten worden gebruikt.

Het **Zweeds initiatief**[5] bevat regels, waaronder termijnen, volgens welke de rechtshandhavingsinstanties van de lidstaten informatie en inlichtingen kunnen uitwisselen teneinde strafrechtelijke onderzoeken of criminele-inlichtingenoperaties uit te voeren. Het hanteert het beginsel van „gelijkwaardige toegang": gegevens moeten aan de verzoekende lidstaat worden verstrekt onder voorwaarden die niet strikter zijn dan die welke op het nationale niveau gelden. De uitgewisselde gegevens moeten ook met Europol en Eurojust worden gedeeld voor zover deze betrekking hebben op strafbare feiten die onder hun mandaat vallen.

In 2012 werd een Zweedse onderneming door een bekende Italiaanse fraudeur opgelicht en ertoe gebracht 65 000 euro op een Italiaanse rekening over te maken. Het Zweedse SPOC (zie punt 3.2 hieronder) ontving via Sirene (zie hieronder) een verzoek van Italië om contact op te nemen met de directeur van de onderneming om na te gaan of de betaling had plaatsgevonden; in dat geval zou Italië het geld bevriezen. Zweden heeft actie ondernomen en in het kader van het Zweedse initiatief binnen 24 uur geantwoord. Door snel op te treden werd de Zweedse politie ingelicht over het feit dat een onderneming het slachtoffer was geworden van fraude, verkregen de Italiaanse autoriteiten de nodige informatie om op te treden en zal het geld waarschijnlijk worden teruggegeven.

[3] Conclusies van de Raad van 30 november 2009, 16637/09.

[4] http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/studies/index_en.htm

[5] Kaderbesluit 2006/960/JBZ van de Raad.

In 2012 legde een uit België afkomstige man op de spoeddienst van een ziekenhuis in de buurt van Parijs verwarde verklaringen af over de wijze waarop hij een ernstige schotwonde had opgelopen. De verklaringen van zijn metgezel leidden onderzoekers naar mogelijke daden in België. Uit initiële onderzoeken bleek dat de man ook in België bekend stond, onder meer voor moord. De Franse autoriteiten hebben in het kader van het Zweedse initiatief onmiddellijk uit eigen beweging informatie verstrekt aan de Belgische politie die snel het verband legde met gebeurtenissen in België twee dagen eerder, waarbij vier gewapende mannen een bediende van een juwelierswinkel hadden ontvoerd. Door politie-ingrijpen waren de mannen op de vlucht geslagen; de mannen konden ontkomen maar een van hen werd geraakt in een vuurgevecht met de politie. Deze informatie heeft de Franse autoriteiten ertoe gebracht de man te bewaken in afwachting van een Europees aanhoudingsbevel, dat nog dezelfde dag in België werd uitgevaardigd en via Sirene aan Frankrijk werd doorgegeven.

Het **Prüm**besluit[6] voorziet in de geautomatiseerde uitwisseling van DNA-profielen, vingerafdrukken en voertuigregistratiegegevens om strafbare feiten te onderzoeken (voor DNA, vingerafdrukken en voertuigregistratiegegevens), strafbare feiten te voorkomen (vingerafdrukken en voertuigregistratiegegevens) en om de openbare veiligheid te handhaven (voertuigregistratiegegevens). De vergelijking van biometrische gegevens (DNA, vingerafdrukken) gebeurt op basis van de „treffer/geen treffer-methode": via een geautomatiseerde vergelijking komt een anonieme „treffer" tot stand wanneer het DNA of de vingerafdrukgegevens waarover de verzoekende staat beschikt, overeenstemmen met de gegevens van een andere lidstaat. De betrokken persoonsgegevens of gegevens van de zaak worden alleen verstrekt als antwoord op een afzonderlijk vervolgverzoek.

In een flat in een Duitse stad werd een dode man gevonden die was neergestoken. Op een deurlijst werd een vingerafdruk gevonden. Een geautomatiseerde Prümopzoeking leidde tot een treffer in de Bulgaarse gegevensbank. De nadere informatie waarom Bulgarije de dag erna werd verzocht, werd binnen drie uur doorgegeven en onmiddellijk in het Schengeninformatiesysteem (SIS – zie hieronder) ingevoerd. 's Anderendaags werd de betrokkene in Oostenrijk aangehouden.

In 2007, bij de start van de Prümuitwisselingen, werd in Wenen apparatuur uit een politiewagen gestolen. Een DNA-spoor uit de wagen stemde overeen met een spoor in een soortgelijke zaak uit de Oostenrijkse gegevensbank, maar het was een Prümtreffer in de Duitse gegevensbank die leidde tot de identificatie van een Poolse serie-inbreker. Er werd een Europees aanhoudingsbevel uitgevaardigd in Oostenrijk. De verdachte werd in Polen aangehouden (door een treffer voor een SIS-signalering) en later in Oostenrijk veroordeeld.

Europol ondersteunt het optreden van de lidstaten en hun onderlinge samenwerking bij de voorkoming en bestrijding van georganiseerde criminaliteit, terrorisme en andere vormen van ernstige criminaliteit (die zijn opgesomd in de bijlage bij het Europolbesluit van de Raad[7]) waarbij twee of meer lidstaten betrokken zijn. Het biedt de lidstaten een platform — via nationale Europoleenheden — om criminele inlichtingen en informatie uit te wisselen. Het Europolinformatiesysteem is een gegevensbank met informatie (183 000 items) die lidstaten verstrekken over grensoverschrijdende criminaliteit die binnen het kader van het Europolmandaat valt, de betrokken personen (41 000) en andere daarmee verband houdende gegevens. Europol gebruikt die voor zijn analyses en de lidstaten kunnen er gebruik van maken voor hun onderzoeken. Sinds 2011 kunnen de lidstaten andere

6 Besluit 2008/615/JBZ van de Raad.

7 2009/371/JBZ.

rechtshandhavingsinstanties dan de nationale Europoleenheden aanwijzen, die toegang krijgen om opzoekingen te doen via de treffer/geen treffer-methode. Analysebestanden maken het Europol mogelijk operationele analyses te maken om grensoverschrijdende onderzoeken te ondersteunen.

Met nagemaakte betaalkaarten werden aan geldautomaten in heel Slovenië grote sommen geld afgehaald. Tegen twee Bulgaarse onderdanen werd een onderzoek ingesteld; het gebruik van het Europolinformatiesysteem leidde tot een treffer waaruit bleek dat een van hen soortgelijke feiten had gepleegd in Frankrijk en Italië. Frankrijk verstrekte het Europolinformatiesysteem gedetailleerde informatie. Door een snelle reactie van Frankrijk via SIENA (zie hieronder), gevolgd door een vergelijking van vingerafdrukken en de opheffing van een verwerkingsbeperking, konden de autoriteiten in Slovenië de gegevens gebruiken als bewijsmateriaal voor de rechter. Het analysebestand van Europol legde verbanden bloot tussen zaken in SI, BG, FR, IE, IT en NO.

Het **Schengeninformatiesysteem (SIS)** bevat signaleringen betreffende personen en voorwerpen. Als compenserende maatregel voor de afschaffing van de binnengrenscontroles wordt het zowel gebruikt binnen het Schengengebied als aan zijn buitengrenzen om een hoog veiligheidsniveau binnen dat gebied te handhaven. Het is een grootschalig systeem (meer dan 43 miljoen signaleringen) dat via de treffer/geen treffer-methode toegankelijk is voor agenten in het veld. Na een treffer (dat wil zeggen dat de gegevens over een persoon of een voorwerp overeenstemmen met een signalering) kan aanvullende informatie worden verkregen via de Sirenebureaus (zie hieronder). Het SIS zal worden vervangen door **SIS II**, dat een aantal verbeteringen zal meebrengen, zoals de mogelijkheid om met elkaar verband houdende signaleringen te koppelen (bv. een signalering over een persoon en over een voertuig), nieuwe categorieën signaleringen en een voorziening om vingerafdrukken, foto's en kopieën van Europese aanhoudingsbevelen op te slaan. In het SIS II-besluit van de Raad[8] worden categorieën signaleringen gedefinieerd om de samenwerking tussen politiële en justitiële autoriteiten in strafzaken te ondersteunen. Daarom zullen alle EU-lidstaten deelnemen aan SIS II en zullen Europol en Eurojust toegang blijven hebben. Het beheer van de centrale onderdelen van SIS II zal worden overgedragen aan het IT-agentschap[9].

Andere EU-instrumenten of IT-systemen voorzien in de uitwisseling van rechtshandhavingsinformatie tussen douaneautoriteiten (de Napels II-overeenkomst; het douane-informatiesysteem als onderdeel van de gegevensbanken van het antifraude-informatiesysteem dat wordt beheerd door het Europees Bureau voor fraudebestrijding – OLAF), financiële-inlichtingeneenheden, bureaus voor de ontneming van vermogensbestanddelen en nationale signaleringsplatforms voor cybercriminaliteit[10]. Rechtshandhavingsinstanties hebben toegang tot andere grootschalige EU-systemen (Visuminformatiesysteem) of die toegang wordt voorgesteld (Eurodac[11]) met het oog op het voorkomen, opsporen en onderzoeken van terrorisme en andere ernstige misdrijven. De vraag of rechtshandhavingsinstanties toegang moeten krijgen en, zo ja, onder welke voorwaarden, is

8 2007/533/JBZ.

9 Europees Agentschap voor het operationele beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht.

10 De verwachte Europese cyberveiligheidsstrategie zal het mogelijk maken de toekomstige behoeften op het gebied van informatie-uitwisseling tussen het netwerk, de instanties voor informatiebeveiliging en de rechtshandhavingsinstanties te evalueren, bv. via het Europees Centrum voor de bestrijding van cybercriminaliteit.

11 EU-gegevensbank met vingerafdrukken van asielzoekers en personen die onregelmatig de grens overschrijden.

ook het voorwerp van de voorbereidende werkzaamheden die thans plaatsvinden met het oog op een voorstel voor een inreis/uitreissysteem dat binnenkort wordt voorgesteld.

Er wordt een Europees grensbewakingssysteem (Eurosur) ontwikkeld voor informatie-uitwisseling en operationele samenwerking tussen de nationale coördinatiecentra en met Frontex om situaties beter te kunnen inschatten en er sneller op te kunnen reageren en zo onregelmatige migratie en grensoverschrijdende criminaliteit aan de buitengrenzen van de EU te voorkomen. Er wordt een gemeenschappelijke gegevensuitwisselingsstructuur (CISE) voor de bewaking van het maritieme gebied van de EU ontwikkeld dat onder meer tot doel heeft het gemeenschappelijk maritiem situationeel bewustzijn te bevorderen om de informatie-uitwisseling tussen openbare instanties in zeven relevante sectoren (waaronder rechtshandhaving in het algemeen) en over de grenzen heen mogelijk te maken en tegelijk interoperabiliteit tot stand te brengen tussen bestaande en toekomstige bewakingssystemen, zoals Eurosur.

De lidstaten wisselen ook informatie uit op grond van het nationale recht en van bilaterale overeenkomsten. Alle lidstaten zijn ook lid van Interpol, waardoor met landen in de hele wereld informatie kan worden uitgewisseld, hetzij via Interpolberichten en –gegevensbanken (bv. gestolen en verloren reisdocumenten) of bilateraal door het Interpolkanaal te gebruiken.

2.2. Kanalen en communicatie-instrumenten

Er **worden drie belangrijke kanalen** gebruikt voor grensoverschrijdende informatie-uitwisseling die alle drie gebaseerd zijn op nationale eenheden in elke lidstaat die gebruikmaken van een gekoppeld communicatie-instrument:

(1) de Sirenebureaus[12] kunnen, na een treffer voor een SIS-signalering, aanvullende informatie verkrijgen van de lidstaat die de signalering heeft aangeleverd. Zij zijn 24 per dag en zeven dagen per week operationeel en volgen de in het Sirenehandboek vastgestelde procedures. Thans wisselen zij informatie uit door gebruik te maken van een systeem dat SISNET wordt genoemd en dat eind maart 2013 zal worden vervangen door het SIS II-communicatienetwerk.

(2) de nationale **Europol**eenheden wisselen informatie uit met Europol. Zij kunnen ook bilateraal informatie uitwisselen over strafbare feiten die niet onder het Europolmandaat vallen en zonder dat Europol daarbij wordt betrokken. De nationale Europoleenheden kunnen rechtstreeks informatie uitwisselen of via Europolverbindingsofficieren, die deel uitmaken van een dergelijke eenheid maar die gedetacheerd zijn bij het hoofdkwartier van Europol. Europol heeft een beveiligd communicatie-instrument, **SIENA**[13], ontwikkeld om informatie uit te wisselen met Europol en tussen de lidstaten. In 2011 hebben de lidstaten SIENA gebruikt om 222 000 berichten uit te wisselen; in 53% van de gevallen werd de informatie uit het bericht gedeeld met Europol.

(3) de nationale centrale bureaus van **Interpol**, die 24 uur per dag en zeven dagen per week operationeel zijn, wisselen informatie uit met Interpol, maar ook bilateraal,

[12] **S**upplementary **I**nformation **RE**quest at the **N**ational **E**ntry (verzoek om aanvullende informatie bij het nationale deel).

[13] **S**ecure **I**nformation **E**xchange **N**etwork **A**pplication (beveiligde netwerktoepassing voor informatie-uitwisseling).

zonder dat Interpol daarbij betrokken wordt. De nationale centrale bureaus gebruiken het door Interpol ontwikkelde communicatie-instrument I-24/7.

Andere kanalen zijn onder de meer de bilaterale verbindingsofficieren (die in andere lidstaten gedetacheerd zijn en typisch worden ingezet in complexere zaken) en de centra voor politiële en douanesamenwerking (die zijn opgericht door aangrenzende lidstaten om de informatie-uitwisseling en de operationele samenwerking in grensgebieden te ondersteunen).

De **keuze van het kanaal** wordt deels door het EU-recht geregeld: SIS-verzoeken om aanvullende informatie na een treffer moeten via de Sirenebureaus worden ingediend en uitwisseling van informatie met Europol moet via de nationale Europoleenheden gebeuren. In andere gevallen kunnen de lidstaten kiezen.

2.3. Interactie tussen de verschillende instrumenten, kanalen en middelen

Er bestaan verscheidene instrumenten, kanalen en middelen, die elk met specifieke doelen zijn ontworpen. In een strafrechtelijk onderzoek kunnen parallel of achtereenvolgens meer dan een instrument worden gebruikt. In een grensoverschrijdende zaak van ernstige of georganiseerde criminaliteit kan een persoon of een voorwerp zowel worden getoetst aan het Europolinformatiesysteem als aan SIS, en wanneer er treffers worden gevonden, kunnen vervolgverzoeken worden ingediend via de kanalen van respectievelijk Europol of Sirene. Een biometrisch spoor kan het voorwerp zijn van een Prümuitwisseling, gevolgd door een post-treffer-verzoek op basis van het Zweedse initiatief met gebruikmaking van het SIENA-instrument.

Welke ook de combinatie of volgorde is, de regels van elk instrument moeten worden nageleefd. Het gaat onder meer om regels inzake gegevensbescherming, beveiliging en kwaliteit van gegevens, en het doel waarvoor de instrumenten mogen worden gebruikt. De nationale verwerking van gegevens voor grensoverschrijdende uitwisseling moet ook in overeenstemming zijn met de EU-wetgeving inzake bescherming van persoonsgegevens[14]. Het evenredigheidsbeginsel moet worden nageleefd; verzoeken op grond van het Zweedse initiatief mogen bijvoorbeeld worden afgewezen wanneer het doorgeven van informatie duidelijk niet in evenredig is met het doel van het verzoek. De eerbiediging van deze regels vereist dat verzoeken en antwoorden worden gevalideerd door goed opgeleid personeel dat werkt met passende informatie-instrumenten.

2.4. Verband met justitiële samenwerking

Bij strafrechtelijke onderzoeken zijn zowel rechtshandhavingsinstanties als gerechtelijke instanties betrokken, maar de lidstaten verschillen onder meer wat betreft de mate waarin het strafrechtelijk onderzoek door gerechtelijke instanties (met inbegrip van de openbare aanklager) wordt geleid of daarop door hen wordt toegezien. Wanneer de gerechtelijke instanties de leiding hebben, alsook wanneer informatie nodig is als bewijsmiddel, zijn typisch justitiële samenwerkingsprocedures op het gebied van wederzijdse rechtshulp vereist.

Voorts kan informatie die in één lidstaat rechtstreeks toegankelijk is voor rechtshandhavingsinstanties, in een andere lidstaat aan gerechtelijke toestemming onderworpen zijn. Het Zweedse initiatief vereist dat, ingeval de gevraagde informatie aan gerechtelijke toestemming is onderworpen, de aangezochte rechtshandhavingsinstantie een

[14] Kaderbesluit 2008/977 van de Raad.

verzoek richt aan de gerechtelijke instantie, die dezelfde regels moet toepassen als in een louter interne zaak.

Uit de inventaris is echter gebleken dat rechtshandhavingsdeskundigen de uiteenlopende regels als een bron van vertraging voor grensoverschrijdende onderzoeken ervaren. Hoewel dat niet binnen het bestek van deze mededeling valt, kan worden opgemerkt dat Eurojust beschikbaar is om justitiële samenwerking te vergemakkelijken. Ook het Europees onderzoeksbevel, dat thans wordt besproken, zou van belang kunnen zijn; het zou de bestaande regels voor grensoverschrijdende bewijsverkrijging kunnen vervangen ter uitvoering van het beginsel van wederzijdse erkenning. Dat bevel zou moeten worden erkend en ten uitvoer gelegd met dezelfde snelheid als in een soortgelijke nationale zaak, en in elk geval binnen bepaalde termijnen.

2.5. Beginselen

In haar overzichtsmededeling van 2010 heeft de Commissie een aantal materiële en procesgerichte beginselen vastgesteld om nieuwe initiatieven te ontwikkelen en huidige instrumenten te evalueren.

De materiële beginselen zijn:

(1) *Waarborging van de grondrechten, in het bijzonder het recht op privacy en gegevensbescherming*. Deze rechten zijn vastgesteld in de artikelen 7 en 8 van het Handvest en in artikel 16 van het Verdrag betreffende de werking van de EU.

(2) *Noodzakelijkheid.* Een beperking van het recht op privacy kan uitsluitend gerechtvaardigd zijn wanneer zij wettig is, een legitiem doel nastreeft en noodzakelijk is in een democratische samenleving.

(3) *Subsidiariteit.*

(4) *Gericht risicobeheer.* Noodzakelijkheidstoetsing en doelbinding zijn van wezenlijk belang.

De procesgerichte beginselen zijn:

(1) *Kosteneffectiviteit*. Dit houdt in dat rekening wordt gehouden met reeds bestaande oplossingen en wordt nagegaan of de doelen van een voorstel kunnen worden bereikt door de bestaande instrumenten beter te gebruiken.

(2) *Bottom-up beleidsontwikkeling.* Een voorbeeld daarvan is de inventaris waardoor rechtshandhavingsdeskundigen betrokken werden bij de voorbereiding van deze mededeling.

(3) *Duidelijke verdeling van verantwoordelijkheden.* In de overzichtsmededeling van 2010 werd opgemerkt dat de lidstaten geen projectleider hadden tot wie zij zich konden wenden voor advies over de tenuitvoerlegging van de Prümbepalingen. In het Prümverslag van de Commissie wordt beschreven hoe deze leemte thans deels wordt ingevuld door ondersteuning bij Europol. Met betrekking tot de idee uit de overzichtsmededeling van 2010 dat het IT-agentschap technisch advies zou kunnen geven, zij opgemerkt dat de prioriteiten van het agentschap momenteel elders liggen.

Naar aanleiding van de driejaarlijkse evaluatie die eind 2015 plaatsvindt, kan dit opnieuw worden bekeken.

(4) Evaluatie- *en vervalbepaling.* De Commissie heeft verslagen opgesteld over het Zweedse initiatief en over Prüm. In deze mededeling wordt daarmee rekening gehouden.

3. BEOORDELING EN AANBEVELINGEN

In dit punt wordt ingegaan op het Zweedse initiatief, het Prümbesluit en het Europolkanaal. Hoewel SIS en het Sirenekanaal een groot volume informatie-uitwisseling voor hun rekening nemen, worden daarover geen aanbevelingen gedaan aangezien reeds ingrijpende wijzigingen worden voorbereid, met name de verwachte overschakeling naar SIS II.

3.1. Het gebruik van de bestaande instrumenten verbeteren

Behalve de verwachte hervorming van Europol is de Commissie op korte termijn niet voornemens wijzigingen van de bovengenoemde EU-instrumenten voor te stellen. Er is evenmin behoefte aan nieuwe instrumenten. Ten eerste **moeten de bestaande instrumenten ten uitvoer worden gelegd**.

Dit geldt met name voor het Prümbesluit. In het Prümverslag van de Commissie dat deze mededeling vergezelt, wordt vastgesteld dat gegevensuitwisseling in het kader van Prüm zeer wordt gewaardeerd voor onderzoeken, maar dat er sprake is van een ernstige achterstand in de tenuitvoerlegging. **Veel lidstaten wisselen nog geen gegevens uit in het kader van het Prümbesluit, ook al was de omzettingstermijn 26 augustus 2011**[15]. De belangrijkste redenen zijn technisch van aard en zijn te wijten aan een gebrek aan personele en financiële middelen in de lidstaten. Gelet op de mogelijkheden van EU-steun (financiering, mobiele competentieteam, helpdesk) lijkt er echter vooral behoefte te zijn aan de politieke wil om het besluit ten uitvoer te leggen. Zoals in het verslag wordt vermeld, zal de Commissie steun blijven verlenen in de vorm van EU-financiering. De context zal echter veranderen in december 2014, wanneer de Commissie inbreukprocedures zal kunnen inleiden. Tot dan zijn de regels voor de controle van nationale tenuitvoerlegging niet van toepassing, aangezien het Prümbesluit, net als het Zweedse initiatief, werd aangenomen onder de voormalige derde pijler.

Wat het **Zweedse initiatief** betreft, oordeelde de Commissie in 2011 dat het instrument zijn volledige potentieel nog niet had gerealiseerd, maar dat het belang ervan zou toenemen[16]. Die beoordeling blijft geldig; nog niet alle lidstaten hebben het initiatief ten uitvoer gelegd[17]. De meeste lidstaten deelden mee dat zij het hebben omgezet in hun nationale wetgeving[18], terwijl andere verklaarden dat zij het niet hoefden om te zetten aangezien hun nationale wetgeving daarmee al in overeenstemming was[19]. Niettemin wordt het initiatief, ondanks de voordelen

---

15 De volgende lidstaten hebben het besluit ten uitvoer gelegd wat betreft:
DNA: BG/CZ/DE/ES/EE/FR/CY/LV/LT/LU/HU/NL/AT/PT/RO/SI/SK/FI;
vingerafdrukken: BG/CZ/DE/EE/ES/FR/CY/LT/LU/HU/NL/AT/SI/SK;
voertuigregistratiegegevens: BE/DE/ES/FR/LT/LU/NL/AT/PL/RO/SI/FI/SE.
Voor meer details, zie het Prümverslag.

16 SEC(2011) 593.

17 De volgende lidstaten moeten nog uitvoeringswetgeving aannemen: BE/EL/IT/LU.

18 BG/CZ/DK/DE/EE/ES/FR/CY/HU/LT/LV/NL/PL/PT/RO/SI/SK/FI/SE.

19 IE/MT/AT/UK.

ervan, zoals het beginsel van gelijkwaardige toegang en de termijnen, in de praktijk nog niet op grote schaal gebruikt. Als reden wordt onder meer aangehaald dat de alternatieven adequaat worden bevonden en dat het verzoekformulier omslachtig is (zelfs in de vereenvoudigde versie van 2010[20]).

De Commissie werd verzocht het nut ervan voor post-treffer-vervolgverzoeken in het kader van het Prümbesluit te onderzoeken[21]. Wanneer nadere informatie nodig is als bewijsmateriaal voor een rechtbank, zal normaal gesproken een verzoek om justitiële samenwerking vereist zijn. Wanneer de informatie echter niet of nog niet als bewijsmateriaal moet dienen, moet het systematische gebruik van het Zweedse initiatief als rechtsgrondslag en SIENA als communicatie-instrument worden bevorderd, zodat de voordelen ervan ten volle kunnen worden benut en de aanpak van de lidstaten op elkaar kan worden afgestemd met één enkele beste praktijk.

Wat **Europol** betreft, heeft een evaluatie van 2012[22] andere vaststellingen bevestigd, namelijk dat de lidstaten niet op een adequate manier informatie delen met Europol (en derhalve ook niet met elkaar). De Commissie zal dit probleem aanpakken in een voorstel tot wijziging van de rechtsgrondslag van Europol. De Raad heeft op zijn beurt de lidstaten verzocht om meer gebruik te maken van het Europolinformatiesysteem[23].

In lijn met het programma van Stockholm heeft de Commissie een studie besteld over de mogelijke invoering van een **Europees indexsysteem van politiegegevens**[24]. Het is de bedoeling tegemoet te komen aan de behoefte, gelet op de toegenomen grensoverschrijdende aard van criminaliteit, van een politieagent in een lidstaat om te weten of een verdachte ook in een andere lidstaat bij de politie bekend staat. Overeenkomstig het beginsel van kosteneffectiviteit is de Commissie van oordeel dat de oprichting van een Europees indexsysteem van politiegegevens **thans niet gerechtvaardigd is** gelet op het feit dat de bestaande instrumenten en middelen, waarmee dat doel via beter of intensiever gebruik geheel of gedeeltelijk zou kunnen worden bereikt, niet ten volle worden benut. Dat geldt in het bijzonder voor het Europolinformatiesysteem (uploaden van relevante gegevens en uitbreiden van de toegang op nationaal niveau), SIS II (het gebruik van relevante signaleringen over personen of voertuigen stimuleren voor toetsingen met het oog op het vervolgen van strafbare feiten en het voorkomen van bedreigingen voor de openbare veiligheid), SIENA (de toegang op nationaal niveau verder ontwikkelen, de koppeling maken met nationale systemen en in voorkomend geval taken automatiseren) en het Prümbesluit (volledig ten uitvoer leggen om de identificatie van criminelen die in verschillende landen actief zijn, te vergemakkelijken).

De lidstaten wordt verzocht:

- het Zweedse initiatief volledig ten uitvoer te leggen, met inbegrip van het beginsel van gelijkwaardige toegang;
- het Prümbesluit volledig ten uitvoer te leggen, met gebruikmaking van de beschikbare EU-steun;

[20] 9512/1/10.
[21] Conclusies van de Raad van 27-28 oktober 2011, 15277/11.
[22] https://www.europol.europa.eu/sites/default/files/publications/rand_evaluation_report.pdf
[23] Conclusies van de Raad van 7-8 juni 2012.
[24] http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/studies/index_en.htm

- voor post-treffer-vervolgverzoeken op grond van het Prümbesluit, het Zweedse initiatief en het SIENA-instrument te gebruiken.

De Commissie zal:

- in EU-financiering blijven voorzien ter ondersteuning van de tenuitvoerlegging van het Prümbesluit;

- tegen december 2014 de voorbereidingen treffen om op dit gebied de regels toe te passen voor het waarborgen van de nationale tenuitvoerlegging van EU-recht.

3.2. De kanalen stroomlijnen en beheren

De keuze van het kanaal. Het feit dat de lidstaten vrij het kanaal kunnen kiezen (behalve de wettelijke vereisten inzake de Sirenebureaus en de nationale Europoleenheden) heeft onder meer als gevolg dat zij in verschillende mate verschillende kanalen gebruiken. Het handboek van goede praktijken ten behoeve van de eenheden voor internationale politiële samenwerking op nationaal niveau (hierna „handboek van 2008" genoemd)[25], dat is opgesteld onder de bescherming van de hoofden van de politie van de EU, bevat criteria dienaangaande[26], maar deze zijn niet bindend en hebben niet tot convergerende nationale werkwijzen geleid. Sommige lidstaten hebben meer systematisch gebruik gemaakt van het Europolkanaal. Andere lidstaten blijven hoofdzakelijk een beroep doen op het Interpolkanaal, dat aantrekkelijk lijkt te zijn, deels door zijn traditionele centrale rol in internationale politiële samenwerking en deels door de ondervonden gebruiksvriendelijkheid. SISNET wordt door sommige lidstaten gebruikt voor niet-SIS-aangelegenheden, bv. verzoeken op grond van het Zweedse initiatief.

De Commissie is ervan overtuigd dat de tijd gekomen is voor een coherentere aanpak in de EU, die het Europolkanaal een centrale rol geeft. Deze aanpak houdt in dat, wanneer er geen kanaal wettelijk is voorgeschreven, **het Europolkanaal met gebruikmaking van het SIENA-instrument het standaardkanaal wordt** tenzij er specifieke redenen zijn om een ander kanaal te gebruiken. Zo zouden bijvoorbeeld verzoeken in het kader van politiële samenwerking die thans worden verzonden via SISNET (dat wordt opgedoekt zodra SIS II van start gaat[27]), in de toekomst via SIENA moeten worden verzonden.

Sommige lidstaten zijn voorstander van een aanpak die een grote flexibiliteit laat in de keuze om verschillende kanalen te gebruiken. De Commissie is het daar niet mee eens. De ontwikkeling door alle lidstaten van nationale bepalingen over de keuze van het kanaal en de convergentie daarvan naar één enkele gedeelde aanpak zou beter zijn dan de huidige versnipperde aanpak. De keuze voor het Europolkanaal is gerechtvaardigd door de voordelen ervan. Europolverbindingsofficieren kan in voorkomend geval worden gevraagd om tussen te komen. SIENA kan worden gebruikt voor directe bilaterale uitwisseling, maar vergemakkelijkt ook het delen van informatie met Europol overeenkomstig de wettelijke vereisten van het Europolbesluit en het Zweedse initiatief. SIENA-berichten zijn gestructureerd, kunnen grote volumes gegevens bevatten en worden uitgewisseld met een hoog beveiligingsniveau. De gegevens zijn beter beschermd wanneer de informatie in een gestructureerde vorm wordt uitgewisseld, bv. door SIENA te gebruiken. De voorgestelde aanpak is volledig in overeenstemming met het verwachte voorstel van de Commissie voor de

[25] 7968/08.

[26] Herhaald in de richtsnoeren voor de tenuitvoerlegging van het Zweedse initiatief, 9512/1/10.

[27] Het SIS II-communicatienetwerk is wettelijk beperkt tot SIS II-gegevens en aanvullende informatie.

hervorming van Europol en met de strategische richtsnoeren van de Europese Raad in het programma van Stockholm, waarin is bepaald: „Europol moet een knooppunt worden voor informatie-uitwisseling tussen de rechtshandhavingsinstanties van de lidstaten, een dienstverlener en een platform voor rechtshandhavingsdiensten".

Beheer van de kanalen. Een systeem met één enkel contactpunt (single point of contact, hierna „SPOC" genoemd) is een „eenloketsysteem" voor internationale politiële samenwerking, dat 24 uur per dagen en zeven dagen per week operationeel is, waarin een lidstaat zijn Sirenebureau, zijn nationale Europoleenheid, zijn nationale centrale bureaus van Interpol en contactpunten voor andere kanalen samenbrengt. De oprichting door elke lidstaat van een SPOC (ook al werd die term niet altijd gebruikt) was in 2007 een conclusie van de derde ronde van wederzijdse-evaluatiebezoeken[28] en werd aanbevolen in het handboek van 2008. De meeste lidstaten hebben diensten voor internationale politiële samenwerking, maar slechts enkele daarvan hebben de kenmerken van een volwaardig SPOC. In 2012 verzocht de Raad de lidstaten „na te gaan wat de mogelijkheden zijn om een eenloketsysteem op te zetten"[29]. De Commissie zou verder willen gaan: om de uitwisseling van rechtshandhavingsinformatie in de EU in het algemeen te verbeteren, zouden **alle lidstaten een eenloketsysteem moeten opzetten** met bepaalde minimumkenmerken.

Wat verzoeken aan een andere lidstaat betreft, zal het samenbrengen van de verschillende kanalen in een enkele organisatorische structuur die de nationale regels inzake keuze van het kanaal volgt, de correcte en consistente keuze van het kanaal en de kwaliteit van de verzoeken waarborgen. De kwaliteit wordt verzekerd door een SPOC dat verzoeken valideert ter bevestiging van het feit dat zij noodzakelijk en passend zijn. Wanneer de informatie niet via het SPOC zelf wordt uitgewisseld (bv. via centra voor politiële en douanesamenwerking of via nationale instellingen die rechtstreeks uitwisselen via SIENA), kan een SPOC de nationale coördinatie waarborgen. Voor inkomende verzoeken moet een SPOC, wanneer dat wettelijk mogelijk is, directe toegang hebben tot nationale gegevensbanken teneinde verzoeken snel te kunnen beantwoorden, met name binnen de termijnen van het Zweedse initiatief. De bepalingen van het Sirenehandboek (bv. over beveiliging, werkstroomsystemen, gegevenskwaliteit en personeel) zouden een basis kunnen zijn voor de organisatie van alle kanalen op een consistente manier. Het delen van middelen, zoals personeel en infrastructuur kan bijdragen tot kostenbesparingen of ten minste tot een betere aanwending van de middelen.

Een SPOC moet alle rechtshandhavingsinstanties omvatten, ook douane. Er moet in samenwerking worden voorzien tussen het SPOC en de nationale coördinatiecentra voor grensbewaking. Wanneer dat verenigbaar is met de nationale rechtssystemen, moeten verbanden worden gemaakt met de gerechtelijke instanties, in het bijzonder wanneer deze toezien op strafrechtelijke onderzoeken.

Steeds meer centra voor politiële en douanesamenwerking[30] wisselen met succes informatie uit op lokaal en regionaal niveau. Jaarlijkse conferenties op EU-niveau maken het mogelijk ervaringen te delen en een gemeenschappelijke aanpak te bespreken. Hoewel het in het algemeen grote aantal uitwisselingen geen betrekking heeft op de meest ernstige en georganiseerde criminaliteit, is het een van de uitdagingen ervoor te zorgen dat informatie in relevante zaken wordt doorgegeven aan het nationale (SPOC) niveau en in voorkomend geval aan Europol. In deze context kijkt de Commissie uit naar de resultaten van het lopende

[28] 13321/3/07.
[29] Conclusies van de Raad van 7-8 juni 2012, 10333/12.
[30] 38 eind 2011.

proefproject (in het kader van een IMS-maatregel) waarbij in een centrum voor politiële en douanesamenwerking SIENA wordt gebruikt.

Het **platform voor informatie-uitwisseling** is een IMS-maatregel onder leiding van Europol om een gemeenschappelijk portaal te ontwikkelen om toegang te krijgen tot bestaande kanalen en systemen, dat ten volle de regels inzake de beveiliging ervan en inzake gegevensbescherming naleeft. De Commissie is van oordeel dat het vergemakkelijken van het gebruik van bestaande kanalen en systemen voordelen heeft, maar dat verder moet worden nagegaan wat de kosten/baten van een platform voor informatie-uitwisseling zijn, wie voor de financiering zou zorgen en hoe het project zou worden beheerd. Bij dat onderzoek moet ook het IT-agentschap worden betrokken[31].

De lidstaten wordt verzocht:

- wanneer er wettelijk geen kanaal is voorgeschreven, het Europolkanaal met gebruikmaking van het SIENA-instrument te gebruiken als het standaardkanaal tenzij er specifieke redenen zijn om een ander kanaal te gebruiken;
- nationale instructies uit te werken voor de keuze van het kanaal;
- mat name, nadat SIS II van start is gegaan en SISNET is opgedoekt, het Europolkanaal en het SIENA-instrument te gebruiken voor uitwisselingen in het kader van politiële samenwerking waarvoor thans SISNET wordt gebruikt;
- voor zover dat nog niet bestaat, één enkel loket als contactpunt op te richten (SPOC) dat alle belangrijke kanalen bundelt, 24/7 beschikbaar is, alle rechtshandhavingsinstanties samenbrengt en toegang heeft tot de nationale gegevensbanken;
- ervoor te zorgen dat via centra voor politiële en douanesamenwerking uitgewisselde informatie indien nodig wordt doorgegeven aan het nationale niveau en, voor zover relevant, ook aan Europol;
- samenwerking op te zetten tussen het SPOC en de nationale coördinatiecentra van Eurosur.

De Raad wordt verzocht:

- de richtsnoeren op EU-niveau te wijzigen om deze in overeenstemming te brengen met de hierboven voorgestelde richtsnoeren in verband met de keuze van het kanaal.

De Commissie zal:

- deelnemen aan de werkzaamheden om de haalbaarheid na te gaan van een platform voor informatie-uitwisseling.

[31] Europees Agentschap voor het operationele beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht.

3.3. Kwaliteit, beveiliging en bescherming van gegevens waarborgen

De waarborgen op het gebied van gegevensbescherming in de bestaande instrumenten moeten zorgvuldig worden nageleefd. Op grond van het voorstel van de Commissie van 25 januari 2012 voor een richtlijn betreffende de nationale verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten[32] zullen de bestaande gegevensbeschermingsregels moeten worden herzien om na te gaan of zij op de richtlijn moeten worden afgestemd.

Een **hoog niveau van gegevensbeveiliging** is noodzakelijk om de integriteit van uitgewisselde persoonsgegevens te beschermen en om ervoor te zorgen dat de lidstaten vertrouwen hebben in de informatie-uitwisseling. Een ketting is maar zo sterk als de zwakste schakel: de lidstaten en de EU-agentschappen moeten ervoor zorgen dat de gegevens worden uitgewisseld over netwerken die zeer goed beveiligd zijn. Het bovengenoemde voorstel voor een richtlijn bevat regels inzake gegevensbeveiliging[33], en op EU-niveau zijn er gedetailleerde beveiligingsregels ter bescherming van vertrouwelijke EU-informatie[34].

Een **gegevenskwaliteit van hoog niveau** is even belangrijk. Het „bedrijfsproces", dat wil zeggen de manier waarop informatie-uitwisseling in de praktijk plaatsvindt, is in deze context relevant. Een aspect daarvan bestaat erin wanneer mogelijk en aangewezen **specifieke taken te automatiseren**. Het opstellen van een verzoek om informatie aan een andere lidstaat vereist bijvoorbeeld dat gegevens die in een nationaal systeem zijn opgeslagen, opnieuw worden ingevoerd in het gebruikte communicatie-instrument; dit manueel doen, kan leiden tot fouten en vergt tijd. Het automatiseren van dergelijke taken zal mogelijk worden door **UMF II**[35], een andere IMS-maatregel. Dit door de EU gefinancierde project onder leiding van Europol heeft als doel een standaardformaat te ontwikkelen voor berichten waarmee om informatie wordt verzocht en waarmee wordt geantwoord. Dit zou de automatisering van gegevensoverdracht tussen verschillende systemen mogelijk maken, bv. nationale systemen voor het beheer van zaken en SIENA. Naast de eventuele kostenbesparingen of ten minste de betere aanwending van middelen, heeft de afschaffing van het manueel herinvoeren van gegevens een dubbel voordeel. Er komen personele middelen vrij voor valideringstaken. Daarnaast leiden een vermindering van het aantal kopieerfouten en het vergemakkelijken van de informatie-uitwisseling door gestructureerde formaten tot een beter gegevensbeschermingsbeheer.

Automatisering van taken wil niet zeggen dat elke politieman in de EU toegang moet krijgen tot alle politie-informatie in de EU. De uitwisseling moet beperkt blijven tot de gegevens die noodzakelijk en passend zijn, en moet aldus worden beheerd dat zij binnen deze beperkingen blijft. **Daarom werken geautomatiseerde opzoekingen, als een manier om capaciteitsproblemen te verhelpen, op grond van de bestaande EU-instrumenten betreffende informatie-uitwisseling volgens de treffer/geen treffer-methode** (bv. SIS, DNA en vingerafdrukken in het Prümbesluit), of anders zijn zij beperkt tot zeer zorgvuldig omschreven soorten gegevens (bv. voertuigregistratiegegevens in het Prümbesluit). Bepaalde taken kunnen en mogen niet worden geautomatiseerd, met name de validering van verzoeken en antwoorden. Dat is bijzonder belangrijk in het kader van het Zweedse initiatief, dat voorschrijft dat verzoeken gerechtvaardigd moeten zijn.

---

32 COM(2012) 10.

33 Artikelen 27 tot en met 29 van het voorstel.

34 Besluit 2011/292/EU van de Raad.

35 **U**niversal **M**essage **F**ormat.

Ten slotte kan de **interoperabiliteit** tussen verschillende nationale systemen en administratieve structuren voordelen opleveren zoals consistente procedures, kortere antwoordtermijnen, betere gegevenskwaliteit en vereenvoudigd ontwerp en ontwikkeling. In het Europese interoperabiliteitskader[36] worden vier interoperabiliteitsniveaus onderscheiden: het technische, het semantische, het organisatorische en het juridische. In UMF II zal het semantische niveau worden ontwikkeld[37]. Afstemmen op gedeelde praktijken (SPOC, keuze van het kanaal) zal het organisatorische niveau bevorderen. Informatie mag echter steeds enkel daadwerkelijk worden uitgewisseld en gebruikt wanneer dat wettelijk is toegestaan.

Europol en de lidstaten wordt verzocht:

- door te gaan met de ontwikkeling van de UMF II-standaard.

3.4. Opleiding en kennis verbeteren

Om rechtshandhavingsfunctionarissen de nodige kennis en vaardigheden te verschaffen om doeltreffend samen te werken, bereidt de Commissie een Europees opleidingsplan rechtshandhaving voor. Uit een inventaris is gebleken dat de EU-instrumenten inzake informatie-uitwisseling in de basisopleiding van rechtshandhavingsinstanties aan bod komen, maar de kwaliteit van de opleiding werd niet beoordeeld. Gespecialiseerde functionarissen zoals die welke in een SPOC werken, hebben een meer diepgaande opleiding nodig. Uitwisselingen van dergelijk personeel worden ook als bevorderlijk beschouwd[38] en moeten worden aangemoedigd.

De lidstaten wordt verzocht:

- ervoor te zorgen dat alle rechtshandhavingsfunctionarissen een passende opleiding krijgen over grensoverschrijdende informatie-uitwisseling;
- uitwisselingen van SPOC-personeel te organiseren.

De Commissie zal:

- ervoor zorgen dat het Europees opleidingsplan rechtshandhaving opleiding over grensoverschrijdende informatie-uitwisseling omvat.

3.5. Financiering

In het kader van het programma „Preventie en bestrijding van criminaliteit” (ISEC) werd EU-financiering toegekend aan informatie-uitwisselingsprojecten zoals UMF II (830 000 EUR) en de tenuitvoerlegging van Prüm (11,9 miljoen EUR). Het fonds zal in 2014-2020 worden vervangen door een EU-fonds voor binnenlandse veiligheid waaronder informatie-uitwisselingsprojecten in de EU ook subsidiabel zullen zijn.

Het fonds voor binnenlandse veiligheid zal gedeeltelijk worden beheerd door de lidstaten onder het zogenaamde „gedeeld beheer” overeenkomstig de **meerjarenprogramma's. Deze**

[36] COM(2010) 744.

[37] In UMF II wordt rekening gehouden met andere werkzaamheden op het gebied van semantiek, zoals de gemeenschappelijke gegevensmodellen die worden ontwikkeld in het kader van het EU-programma voor interoperabiliteitsoplossingen voor Europese overheidsdiensten.

[38] 10333/12.

programma's zouden rekening moeten houden met de nationale prioriteiten op het gebied van informatie-uitwisseling in lijn met de aanbevelingen in deze mededeling. De Commissie zal tegelijk nagaan hoe onderdelen van het fonds voor binnenlandse veiligheid die onder haar rechtstreeks beheer staan, vooral proefprojecten zouden kunnen ondersteunen, bv. door UMF II verder te ontwikkelen.

Wat de eigen uitgaven van de lidstaten betreft, kunnen andere aanbevelingen (over SPOC, UMF II) zoals aangegeven bijdragen tot kostenbesparingen of ten minste tot een betere aanwending van middelen.

De lidstaten wordt verzocht:

- rekening te houden met de prioriteiten op het gebied van informatie-uitwisseling in nationale meerjarenprogramma's in het kader van het EU-fonds voor binnenlandse veiligheid 2014-2020.

De Commissie zal:

- het beleid inzake informatie-uitwisseling opnemen in de dialogen over de programmering van het EU-fonds voor binnenlandse veiligheid met de lidstaten;
- oproepen tot het indienen van voorstellen doen voor directe financiering (van de Commissie) van relevante proefprojecten.

3.6. Statistieken

De bestaande statistieken zijn weliswaar goed op bepaalde gebieden (bv. SIS, SIENA), maar zijn niet allesomvattend. Betere statistieken zouden leiden tot betere kennis over het gebruik van het Zweedse initiatief (waarvoor alleen cijfers over het gebruik van SIENA bekend zijn) en Prüm.

Statistieken verzamelen kan echter zeer veel middelen vereisen, vooral wanneer dat niet tot de normale werkstroom behoort. Ad-hocoefeningen moeten worden vermeden. Een evolutionaire aanpak is de beste, voortbouwend op reeds begonnen processen, bv., zoals beschreven in het Prümverslag, het bepalen van het aantal Prümtreffers dat daadwerkelijk in onderzoeken is gebruikt. Meer gebruik maken van SIENA voor verzoeken in het kader van het Zweedse initiatief, zoals hierboven aanbevolen, zal ertoe leiden dat meer van die verzoeken zullen verschijnen in de statistieken over SIENA.

De lidstaten wordt verzocht:

- de Prümstatistieken te verbeteren.

4. CONCLUSIES

De grensoverschrijdende informatie-uitwisseling verbeteren, is geen doel op zich. Het doel is criminaliteit doeltreffender aan te pakken en op die manier de schade voor slachtoffers en voor de EU-economie te beperken.

In het algemeen werkt grensoverschrijdende informatie-uitwisseling goed en levert zij, zoals blijkt uit de hierboven gegeven voorbeelden, een uiterst waardevolle bijdrage aan de strijd

tegen ernstige en grensoverschrijdende criminaliteit in de EU. Er is echter ruimte voor verbetering. Wetgeving die is overeengekomen, moet volledig ten uitvoer worden gelegd, door alle lidstaten. Wat de toekomst betreft, moeten de lidstaten in het bijzonder meer systematisch gebruikmaken van het Europolkanaal en moeten alle lidstaten een allesomvattend nationaal eenloketsysteem ontwikkelen (SPOC).

De Commissie zal op haar beurt blijven nagaan hoe de instrumenten ten uitvoer worden gelegd en gebruikt, in EU-financiering blijven voorzien en de verschillende aspecten blijven samenbrengen om consistentie te waarborgen. De Commissie stelt thans geen nieuw instrument voor. Als dat in de toekomst toch gebeurt, dat zal dat in overeenstemming zijn met de materiële beginselen uit de overzichtsmededeling van 2010: waarborgen van de grondrechten en garanderen van noodzakelijkheid, subsidiariteit en gericht risicobeheer.

Er moet nog een grote inspanning worden geleverd om ervoor te zorgen dat relevante informatie met Europol wordt gedeeld om een beeld te krijgen van de grensoverschrijdende criminaliteit in de hele EU. Het komende voorstel van de Commissie over de hervorming van Europol komt daaraan tegemoet. De informatieverstrekking aan Europol zou echter al worden vergemakkelijkt als de aanbevelingen in deze mededeling, namelijk meer systematisch gebruik van het Europolkanaal en zijn instrument voor beveiligde communicatie SIENA, zouden worden gevolgd.

Als follow-up van deze mededeling zal de Commissie met de lidstaten blijven samenwerken in de context van de strategie voor het beheer van rechtshandhavingsinformatie voor interne veiligheid in de EU en stelt zij voor dat de Raad een jaarlijks debat houdt in zijn Comité binnenlandse veiligheid. De Commissie verzoekt ook het Europees Parlement om deze aanbevelingen te bespreken, onder meer in zijn Bijzondere Commissie georganiseerde misdaad, corruptie en witwassen.