EUROPESE
COMMISSIE

Brussel, 6.4.2016
COM(2016) 205 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

Krachtigere en slimmere informatiesystemen voor grenzen en veiligheid

1. INLEIDING

Europa is een mobiele samenleving. Dagelijks overschrijden miljoenen EU-burgers en onderdanen van derde landen de binnen- en buitengrenzen. In 2015 hebben meer dan 50 miljoen onderdanen van derde landen de EU bezocht, goed voor meer dan 200 miljoen grensoverschrijdingen aan de buitengrenzen van het Schengengebied.

Naast deze reguliere reizigersstromen hebben het conflict in Syrië en crises elders, alleen al in 2015 geleid tot 1,8 miljoen irreguliere grensoverschrijdingen aan de buitengrenzen van Europa. EU-burgers verwachten dat personencontroles aan de buitengrenzen doeltreffend zijn, een doeltreffend beheer van migratie mogelijk maken en bijdragen tot de interne veiligheid. De terroristische aanslagen in Parijs in 2015 en in Brussel in maart 2016 hebben de voortdurende dreiging voor de interne veiligheid in Europa scherp aangetoond.

Beide elementen hebben sterker de aandacht gevestigd op de noodzaak om de EU-samenwerkingskaders voor grensbeheer, migratie en veiligheid te bundelen en te versterken. Grensbeheer, rechtshandhaving en migratiebeheer zijn dynamisch met elkaar verbonden. Er zijn gevallen bekend van EU-burgers die de buitengrens hebben overschreden om voor terroristische doeleinden naar conflictgebieden te reizen en die bij terugkeer een gevaar vormen. Er zijn aanwijzingen dat terroristen irreguliere migratieroutes hebben gebruikt om de EU binnen te komen en zich vervolgens ongemerkt binnen het Schengengebied hebben verplaatst.

De Europese agenda's voor veiligheid en migratie hebben de richting aangegeven voor de ontwikkeling en uitvoering van het EU-beleid voor de aanpak van de parallelle uitdagingen van migratiebeheer en strijd tegen terrorisme en georganiseerde criminaliteit. Deze mededeling bouwt voort op de synergieën tussen deze twee agenda's en is bedoeld als uitgangspunt voor een discussie over de vraag hoe bestaande en toekomstige informatiesystemen zowel het beheer van de buitengrenzen als de interne veiligheid van de EU kunnen bevorderen. Zij is een aanvulling op het voorstel van december 2015 over de oprichting van een Europese grens- en kustwacht en de verbetering van crisispreventie en interventie aan de buitengrenzen.

Op EU-niveau bestaat een aantal informatiesystemen dat grenswachten en politiefunctionarissen van relevante informatie over personen voorziet, maar de EU-architectuur voor gegevensbeheer is niet perfect. Deze mededeling schetst een aantal opties om de voordelen van bestaande informatiesystemen te optimaliseren en, indien nodig, nieuwe en aanvullende maatregelen te nemen om lacunes aan te pakken. Ook wordt daarin de aandacht gevestigd op de noodzaak om als langetermijndoelstelling de interoperabiliteit van informatiesystemen te verbeteren, welke noodzaak ook is vastgesteld door de Europese Raad en de Raad[1], en worden daarin ideeën voorgesteld over de manier waarop in de toekomst informatiesystemen kunnen worden ontwikkeld om ervoor te zorgen dat grenswachten, douanebeambten, politiefunctionarissen en justitiële autoriteiten over de nodige informatie kunnen beschikken.

Elk toekomstig initiatief zou worden opgesteld op basis van de beginselen van betere regelgeving en vergezeld gaan van een openbare raadpleging en een effectbeoordeling,

[1] Conclusies van de Europese Raad van 17 en 18 december 2015; Gezamenlijke verklaring van de EU-ministers van Justitie en Binnenlandse Zaken en van de vertegenwoordigers van de EU-instellingen over de terreuraanslagen op 22 maart 2016 in Brussel (24 maart 2016); Conclusies van de Raad van de EU en van de lidstaten in het kader van de Raad bijeen inzake terrorismebestrijding (20 november 2015).

onder meer wat betreft de grondrechten, en met name het recht op de bescherming van persoonsgegevens.

2. UITDAGINGEN

Het ontbreken van binnengrenzen in het Schengengebied vereist een sterk en betrouwbaar beheer van het verkeer van personen over de buitengrenzen. Dit is een noodzakelijke voorwaarde om een hoog niveau van interne veiligheid en het vrij verkeer van personen binnen dat gebied te waarborgen. Tegelijkertijd betekent het ontbreken van binnengrenzen dat rechtshandhavingsinstanties in de lidstaten ook toegang krijgen tot relevante persoonsgegevens. Er bestaat een aantal informatiesystemen en gegevensbanken op EU-niveau die grenswachten, politiefunctionarissen en andere instanties voorzien van relevante informatie over personen, overeenkomstig hun respectieve doeleinden[2].

Informatiesystemen vertonen echter ook tekortkomingen die het werk van deze nationale instanties hinderen. Daarom werd betere informatie-uitwisseling een belangrijke prioriteit in de Europese veiligheidsagenda. De belangrijkste tekortkomingen zijn: a) suboptimale werking van bestaande informatiesystemen, (b) lacunes in de EU-architectuur voor gegevensbeheer, (c) een complex landschap van op verschillende wijze beheerde informatiesystemen, en (d) een gefragmenteerde architectuur van gegevensbeheer voor grenstoezicht en veiligheid.

De bestaande informatiesystemen in de EU voor grensbeheer en interne veiligheid bestrijken een breed gamma van functies. Toch zijn er nog steeds **tekortkomingen in de functies van de bestaande systemen**. Wanneer naar de grenstoezichtprocessen voor verschillende categorieën reizigers wordt gekeken, blijkt duidelijk dat er tekortkomingen zijn in sommige van deze processen en tussen de respectieve informatiesystemen voor grenstoezicht. Zo moet ook de doeltreffendheid van de bestaande instrumenten voor rechtshandhaving worden geoptimaliseerd. Dit pleit voor het bestuderen van maatregelen ter verbetering van de bestaande informatiesystemen (punt 5).

Bovendien zijn er lacunes in de **EU-architectuur voor gegevensbeheer**. Er blijven problemen voor grenscontroles voor specifieke categorieën reizigers, zoals onderdanen van derde landen met een visum voor verblijf van langere duur. Ook is er een gebrek aan informatie vóór aankomst aan de grenzen wat betreft onderdanen van derde landen die van de visumplicht zijn vrijgesteld. Er moet aandacht worden besteed aan de vraag of het nodig is om die lacunes op te vullen door zo nodig aanvullende informatiesystemen te ontwikkelen (punt 6).

Grenswachten en met name politiefunctionarissen worden geconfronteerd met een **complex landschap van op verschillende wijze beheerde informatiesystemen** op EU-niveau. Deze complexiteit leidt tot praktische moeilijkheden, met name over de vraag welke gegevensbanken in een bepaalde situatie specifiek moeten worden gecontroleerd. Bovendien zijn niet alle lidstaten op alle bestaande systemen aangesloten[3]. De huidige complexiteit wat de toegang tot informatiesystemen op EU-niveau betreft, kan worden beperkt door de invoering van één enkele zoekinterface op nationaal niveau waarbij rekening wordt gehouden met de verschillende doeleinden van toegang (punt 7.1).

---

[2] Zie punt 4 voor een overzicht van informatiesystemen betreffende grenzen en veiligheid, en bijlage 2 voor een uitvoeriger inventaris.

[3] Behoudens de bijzondere bepalingen van protocol nr. 22 wat Denemarken betreft en de protocollen nrs. 21 en 36 wat het Verenigd Koninkrijk en Ierland betreft, en de respectieve toetredingsakten.

De huidige EU- architectuur voor gegevensbeheer voor grenstoezicht en veiligheid wordt gekenmerkt door **fragmentatie**. Dit is een gevolg van de verschillende institutionele, juridische en politieke context waarin de systemen zijn ontwikkeld. Informatie wordt afzonderlijk opgeslagen in verschillende systemen, die zelden met elkaar verbonden zijn. Er is sprake van inconsistentie tussen gegevensbanken en de betrokken instanties hebben niet dezelfde toegang tot gegevens. Dit kan met name voor rechtshandhavingsinstanties leiden tot blinde vlekken, aangezien het zeer moeilijk kan zijn om verbanden tussen deelgegevens te herkennen. Het is derhalve noodzakelijk en dringend om te werken aan geïntegreerde oplossingen voor een betere toegankelijkheid tot gegevens voor grensbeheer en -beveiliging, met volledige inachtneming van de grondrechten. Daarom is het nodig een proces op gang te brengen met het oog op de interoperabiliteit van de bestaande informatiesystemen (punt 7).

3. GRONDRECHTEN

Volledige inachtneming van de grondrechten en de gegevensbeschermingsregels is een essentiële voorwaarde om elk van de genoemde problemen aan te pakken.

Inachtneming van de grondrechten vereist goed opgezette en correct gebruikte technologie en informatiesystemen. Technologie en informatiesystemen kunnen overheidsinstanties helpen de grondrechten van de burgers te beschermen. De biometrische technologie kan het risico van identificatiefouten, discriminatie en raciale profilering beperken. Zij kan ook bijdragen tot het aanpakken van de risico's inzake de bescherming van kinderen, zoals kinderen die vermist raken of het slachtoffer worden van mensenhandel, op voorwaarde dat zij gepaard gaat met waarborgen op het gebied van grondrechten en beschermingsmaatregelen. Biometrische technologie kan het risico verminderen dat personen ten onrechte worden aangehouden en gevangengenomen. Zij kan ook bijdragen aan een grotere veiligheid voor burgers die in het Schengengebied verblijven, omdat zij zal helpen bij de bestrijding van terrorisme en zware criminaliteit.

Het bestaan van grootschalige informatiesystemen houdt ook potentiële risico's in voor de privacy, waarop moet worden geanticipeerd en die naar behoren moeten worden aangepakt. Het verzamelen en het gebruik van persoonsgegevens in die systemen heeft gevolgen voor het recht op privacy en de bescherming van persoonsgegevens, zoals vastgelegd in het Handvest van de grondrechten van de Europese Unie. Alle systemen moeten in overeenstemming zijn met de beginselen van gegevensbescherming en de vereisten van noodzakelijkheid, evenredigheid, doelbinding en gegevenskwaliteit. Er moeten waarborgen zijn voor de rechten inzake de bescherming van de persoonlijke levenssfeer en persoonsgegevens van de betrokkenen. Gegevens mogen alleen worden bewaard zolang dat nodig is voor het doel waarvoor zij werden verzameld. Er moet worden voorzien in mechanismen voor een accuraat risicobeheer en een effectieve bescherming van de rechten van de betrokkenen.

In december 2015 hebben de medewetgevers een politiek akkoord bereikt over de hervorming van de gegevensbescherming. Na goedkeuring zullen de nieuwe algemene verordening gegevensbescherming en de richtlijn inzake gegevensbescherming voor politiële en strafrechtelijke autoriteiten[4] in 2018 van toepassing worden en een geharmoniseerd kader bieden voor de verwerking van persoonsgegevens.

Doelbinding is een belangrijk beginsel van gegevensbescherming zoals vastgelegd in het Handvest van de grondrechten. Als gevolg van de verschillende institutionele, juridische en

[4] Zie http://ec.europa.eu/justice/data-protection/reform/index_en.htm

politieke contexten waarin informatiesystemen op EU-niveau zijn ontwikkeld, werd aan het beginsel van doelbinding uitvoering gegeven via een gecompartimenteerde structuur van informatiebeheer[5]. Dit is een van de redenen voor de huidige fragmentatie van de EU-architectuur voor gegevensbeheer inzake grenstoezicht en interne veiligheid. Op grond van het nieuwe algemene kader voor de bescherming van persoonsgegevens in de EU en belangrijke ontwikkelingen in de technologie en IT-beveiliging, kan aan het beginsel van doelbinding gemakkelijker uitvoering worden gegeven wat betreft de toegang tot en het gebruik van de opgeslagen gegevens, met volledige inachtneming van het Handvest van de grondrechten en van de recente jurisprudentie van het Hof van Justitie van de Europese Unie. Waarborgen zoals het compartimenteren van gegevens binnen één systeem en specifieke regels inzake toegang en gebruik voor elke categorie gegevens en gebruikers moeten zorgen voor de noodzakelijke doelbeperking binnen geïntegreerde oplossingen voor gegevensbeheer. Dit biedt mogelijkheden voor de interoperabiliteit van informatiesystemen, gepaard aan de noodzakelijke strikte voorschriften betreffende toegang en gebruik zonder afbreuk te doen aan de bestaande doelbeperking van het doel.

"Ingebouwde gegevensbescherming" en "gegevensbescherming door standaardinstellingen" zijn nu uitgangspunten voor de EU-voorschriften inzake gegevensbescherming. Bij de ontwikkeling van nieuwe instrumenten waarbij gebruik wordt gemaakt van informatietechnologie, zal de Commissie trachten deze aanpak te volgen. 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[6].

De dwingende bepalingen van het Handvest van de grondrechten en in het bijzonder de nieuwe instrumenten voor de hervorming van de gegevensbescherming zullen de voor de Commissie leidend zijn bij de aanpak van de huidige lacunes en tekortkomingen in de EU-architectuur voor gegevensbeheer inzake grenstoezicht en veiligheid. Dit zal ervoor zorgen dat de verdere ontwikkeling van informatiesystemen op deze gebieden in overeenstemming zal zijn met de allerstrengste normen voor gegevensbescherming, en dat deze systemen de door het Handvest van de grondrechten gewaarborgde grondrechten zullen eerbiedigen.

---

5 COM(2010) 385 def.

6 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.

4. OVERZICHT VAN INFORMATIESYSTEMEN VOOR GRENZEN EN VEILIGHEID[7]

De bestaande informatiesystemen in de EU voor grensbeheer en interne veiligheid hebben elk hun eigen doelstellingen, rechtsgronden[8], gebruikersgroepen en institutionele context. Samen vormen zij een complex patroon van gegevensbanken.

De drie belangrijkste door de EU ontwikkelde **gecentraliseerde informatiesystemen** zijn: i) het Schengeninformatiesysteem (SIS) met een breed scala van signaleringen van personen en voorwerpen, (ii) het Visuminformatiesysteem (VIS) met gegevens over visa voor kort verblijf, en (iii) het Eurodac-systeem met vingerafdrukken van asielzoekers en onderdanen van derde landen die de buitengrens irregulier hebben overschreden. Deze drie systemen zijn complementair en zijn — met uitzondering van het SIS — vooral gericht op onderdanen van derde landen. De systemen bieden de nationale autoriteiten ook ondersteuning in de bestrijding van misdaad en terrorisme[9]. Dit geldt met name voor het SIS, momenteel het meest gebruikte instrument voor informatie-uitwisseling. In het kader van deze systemen vindt de gegevensuitwisseling plaats via een beveiligde en specifieke communicatie-infrastructuur, sTESTA genoemd[10].

Naast deze bestaande systemen, stelt de Commissie voor een vierde gecentraliseerd grensbeheersysteem op te richten, het inreis-uitreissysteem (EES)[11], dat naar verwachting tegen 2020 zal zijn geïmplementeerd en ook op onderdanen van derde landen gericht zal zijn.

---

7 Zie bijlage 2 voor een overzicht van de bestaande informatiesystemen voor grensbeheer en rechtshandhaving.

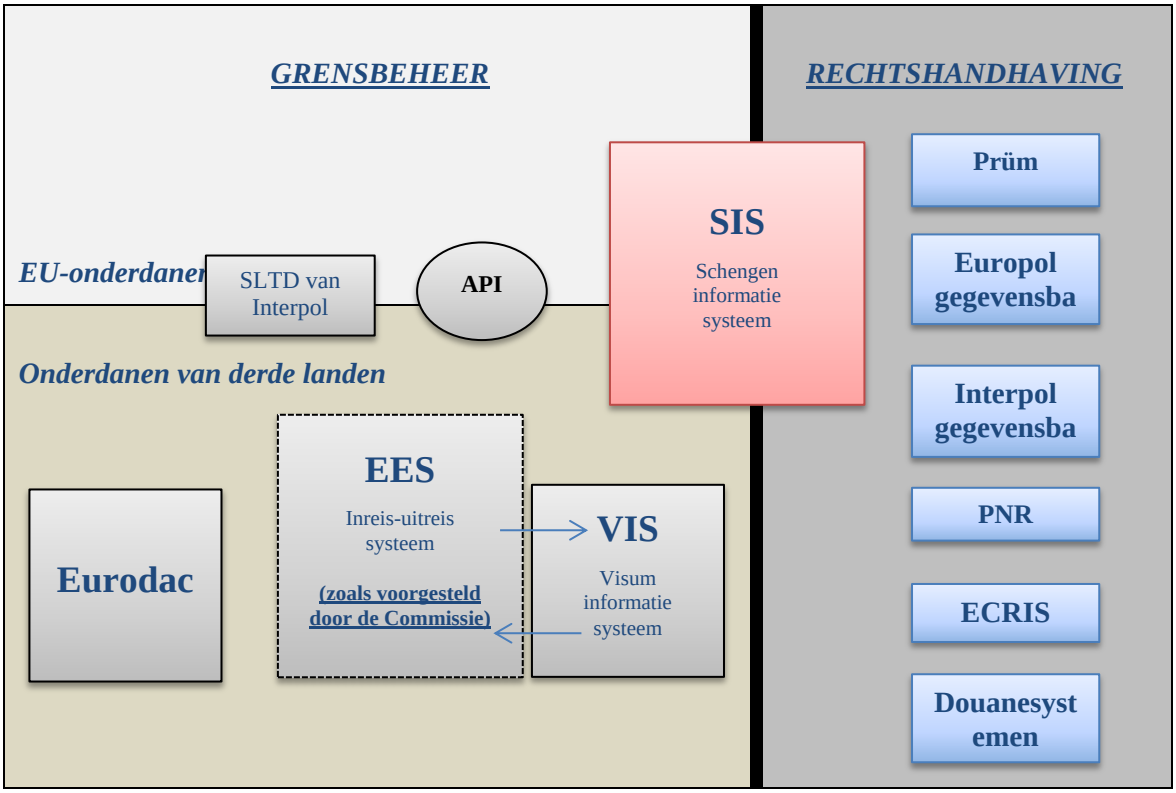
8 Behoudens de bijzondere bepalingen van protocol nr. 22 wat Denemarken betreft en de protocollen nrs. 21 en 36 wat het Verenigd Koninkrijk en Ierland betreft.

9 De toegang van rechtshandhavingsinstanties tot het VIS en Eurodac is in beperkte omstandigheden mogelijk, aangezien rechtshandhaving slechts een ondergeschikt doel is van deze systemen. In het kader van het VIS moeten de lidstaten een instantie aanwijzen die verantwoordelijk is om de toegang van rechtshandhavingsinstanties te controleren en moet de politie bewijzen dat hun toegang noodzakelijk is voor strafrechtelijk onderzoek. Wat Eurodac betreft, moet de onderzoeksinstantie eerst het nationale AFIS, Prüm en het VIS doorzoeken alvorens toegang te krijgen tot Eurodac.

10 Wordt binnenkort vervangen door TESTA-NG.

11 COM(2016) 194 final.

Figuur 1 *Schematisch overzicht van de belangrijkste informatiesystemen voor grensbeheer en rechtshandhaving:*



Andere bestaande instrumenten voor grensbeheer zijn de Interpol-gegevensbank voor gestolen en verloren reisdocumenten (SLTD) en het Advance Passenger Information (API) waarmee informatie over passagiers wordt verzameld voordat zij een vlucht naar de EU nemen. Deze instrumenten zijn relevant voor zowel EU-burgers als onderdanen van derde landen.

Specifiek voor rechtshandhaving, strafrechtelijk onderzoek en justitiële samenwerking heeft de EU **gedecentraliseerde instrumenten voor informatie-uitwisseling** ontwikkeld, namelijk (i) het kader van Prüm voor de uitwisseling van DNA, vingerafdrukken en gegevens uit kentekenregisters, en (ii) het Europees Strafregister Informatiesysteem (Ecris) waarmee gegevens uit nationale strafregisters worden uitgewisseld. Ecris maakt, via een beveiligd netwerk, de uitwisseling van informatie mogelijk over eerdere veroordelingen van een specifieke persoon door de strafrechter in de Europese Unie. De verzoeken berusten hoofdzakelijk op alfanumerieke identiteitsinformatie, al is ook de uitwisseling van biometrische gegevens mogelijk.

Europol ondersteunt, als EU-informatiecentrum op het gebied van criminaliteit, de uitwisseling van informatie tussen nationale politiediensten. Het Europol-informatiesysteem (EIS) biedt de lidstaten een gecentraliseerde gegevensbank voor informatie over criminaliteit waar zij gegevens over zware criminaliteit en terrorisme kunnen opslaan en raadplegen. Contactpunten bij Europol bieden werkbestanden met een onderwerpgerichte analyse met informatie over lopende operaties in de lidstaten. De Europol-applicatie voor veilige informatie-uitwisseling (SIENA) biedt lidstaten de mogelijkheid om op een snelle, veilige en gebruiksvriendelijke manier informatie uit te wisselen met elkaar, met Europol of met derden die een samenwerkingsovereenkomst met Europol hebben. Tegelijkertijd is SIENA sterk gericht op interoperabiliteit met andere Europol-systemen, bijvoorbeeld het systeem voor rechtstreekse uitwisseling van informatie met contactpunten. Het biedt de mogelijkheid de gegevensbanken van Europol te voeden met informatie die tussen de

lidstaten wordt uitgewisseld. SIENA zou daarom het voorkeurskanaal van de lidstaten moeten zijn voor de uitwisseling van informatie in de EU in het kader van rechtshandhaving.

Het **Passenger Name Records** (PNR)-systeem vormt nog een reeks van systemen voor de verwerking van persoonsgegevens die in de lidstaten zullen worden ontwikkeld[12]. PNR-gegevens bestaan uit de informatie die bij de boeking of het inchecken wordt verstrekt.

Ten slotte zijn ook de **douaneautoriteiten** een cruciale speler binnen de multi-institutionele samenwerking aan de buitengrenzen. Zij beschikken over verschillende systemen[13] en gegevensbanken die gegevens bevatten over de verplaatsing van goederen, identificatie van marktdeelnemers en risicogerelateerde informatie die kunnen worden gebruikt om de interne veiligheid te versterken. Deze systemen hebben ook hun eigen gecontroleerde, beperkte en beveiligde infrastructuur (Common Communication Network) die heeft bewezen levensvatbaar te zijn. Er moet verder worden gezocht naar synergieën en convergentie tussen informatiesystemen en de bijbehorende infrastructuur ten behoeve van het EU-grensbeheer en douaneverrichingen.

5. DE BESTAANDE INFORMATIESYSTEMEN VERBETEREN

De bestaande informatiesystemen in de EU voor grensbeheer en interne veiligheid bestrijken een breed gamma van functies. De systemen vertonen echter nog **tekortkomingen** die moeten worden aangepakt om de prestaties ervan te optimaliseren.

Schengeninformatiesysteem (SIS)

Grenscontroles met het **Schengeninformatiesysteem** (SIS) vinden thans plaats op basis van alfanumerieke opzoekingen (d.w.z. naam en geboortedatum). Vingerafdrukken kunnen alleen worden gebruikt voor het verifiëren en bevestigen van de identiteit van een persoon die reeds is vastgesteld op basis van diens naam. Door deze beveiligingslacune kunnen personen die gesignaleerd staan, gebruik maken van valse documenten om te ontkomen aan een exacte match in het SIS.

Deze kritieke tekortkoming zal worden aangepakt door aan het SIS een zoekfunctie voor vingerafdrukken toe te voegen via een **geautomatiseerd identificatiesysteem voor vingerafdrukken (AFIS)**, zoals bepaald in het bestaande rechtskader[14]. Het AFIS zou medio 2017 operationeel moeten zijn[15]. Zodra het AFIS is ontwikkeld, zal het toegankelijk zijn voor Europol en op die manier een aanvulling vormen op de Europol-

---

[12] Zie punt 6.2.

[13] De douane-informatiesystemen omvatten alle systemen die zijn opgericht in het kader van het communautair douanewetboek (Verordening 2913/92), het toekomstige douanewetboek van de Unie (Verordening 952/2013) en de beschikking betreffende een papierloze omgeving voor douane en bedrijfsleven (Beschikking nr. 70/2008/EG), en het douane-informatiesysteem werd opgericht in het kader van de DIS-Overeenkomst van 1995. Deze hebben als doel bij te dragen tot de bestrijding van douanedelicten door de samenwerking tussen Europese douaneautoriteiten te vergemakkelijken.

[14] Artikel 22, onder c), van Verordening (EG) nr. 1987/2006 van het Europees Parlement en de Raad van 20 december 2006 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) en Besluit nr. 533/2007/JBZ van de Raad van 12 juni 2007 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) (PB L 381 van 28.12.2006, blz. 4, en PB L 2015 van 7.8.2007, blz. 63).

[15] In maart 2016 heeft de Commissie een verslag aan het Europees Parlement en de Raad gepresenteerd over de beschikbaarheid en geschiktheid van technologie voor de identificatie van een persoon op basis van vingerafdrukken die zijn opgeslagen in het Schengeninformatiesysteem van de tweede generatie (SIS II).

systemen voor strafrechtelijk onderzoek en terrorismebestrijding, alsook op de uitwisseling van vingerafdrukken in het kader van Prüm. De Commissie en eu-LISA zullen het potentieel van een dergelijk ruimer gebruik van het AFIS-systeem onderzoeken.

Op basis van de lopende evaluatie en een technische studie onderzoekt de Commissie momenteel **mogelijke aanvullende functies van het SIS** met het oog op het indienen van voorstellen tot herziening van de rechtsgrondslag van het SIS. Aspecten die worden onderzocht, zijn:

- de invoering van signaleringen in het SIS over irreguliere migranten ten aanzien van wie terugkeerbesluiten zijn genomen;
- het gebruik van gezichtsopnamen voor biometrische identificatie, naast vingerafdrukken;
- de automatische toezending van informatie over een treffer na een controle;
- het opslaan van informatie over treffers voor signaleringen met het oog op onopvallende en gerichte controles in het centraal systeem van het SIS.
- de oprichting van een nieuwe signaleringscategorie voor "gezochte onbekende personen" waarvoor mogelijk forensische gegevens beschikbaar zijn in nationale gegevensbanken (bv. een latente vingerafdruk die is achtergelaten op de plaats van het delict)[16].

De Commissie zal met EU-financiering steun blijven verlenen aan de uitvoering van projecten waarmee gelijktijdige opzoekingen mogelijk worden in SIS en de Interpol-gegevensbanken voor gestolen en verloren reisdocumenten (SLTD) en voor gezochte criminelen, voertuigen of vuurwapens (iARMS), die complementair zijn met de EU-informatiesystemen[17].

De Interpol-gegevensbank voor gestolen en verloren reisdocumenten (SLTD)

Het is van essentieel belang voor een doeltreffend grensbeheer dat de reisdocumenten van alle onderdanen van derde landen en EU-burgers getoetst worden aan de **SLTD-gegevensbank**. Ook rechtshandhavingsinstanties zouden de SLTD-gegevensbank moeten gebruiken voor zoekopdrachten binnen het Schengengebied. Naar aanleiding van de terroristische aanslagen in Parijs op 13 november 2015 vroeg de Raad om elektronische verbindingen met de relevante gegevensbanken van Interpol op alle grensdoorlaatposten en automatische controle van reisdocumenten tegen maart 2016[18]. Alle lidstaten zouden moeten zorgen voor de betrokken elektronische verbindingen en systemen moeten opzetten waarmee gegevens over gestolen of verloren reisdocumenten in de SLTD-gegevensbank automatisch kunnen worden bijgewerkt.

Advance Passenger Information (API)

In aansluiting op bestaande goede praktijken zouden de lidstaten ook moeten zorgen voor een grotere meerwaarde van gegevens uit het **Advance Passenger Information** (API)-systeem, door te voorzien in geautomatiseerde kruiscontrole van deze gegevens met het SIS en de SLTD-gegevensbank van Interpol. De Commissie zal nagaan of het nodig is om de rechtsgrondslag voor de verwerking van API-gegevens te herzien met het oog op

[16] Het instellen van deze nieuwe signalering zal worden beoordeeld om te zoeken naar complementariteit en overlapping te vermijden met het bestaande Prüm-kader voor het zoeken naar vingerafdrukken in de verschillende nationale gegevensbanken van de EU-lidstaten.

[17] Door Interpol ontwikkelde instrumenten om informatie te zoeken, zoals de Fixed Interpol Networked Database (FIND) en de Mobile Interpol Networked Database (MIND), hebben als doel gelijktijdige opzoekingen in de Interpol-systemen en in het SIS mogelijk te maken.

[18] Conclusies van de Raad van de EU en van de lidstaten in het kader van de Raad bijeen inzake terrorismebestrijding, 20 november 2015.

een bredere tenuitvoerlegging en om de lidstaten te verplichten om voor alle inkomende en uitgaande vluchten API-gegevens te verlangen en te gebruiken. Dit is met name van belang in het kader van de tenuitvoerlegging van de toekomstige richtlijn inzake persoonsgegevens van passagiers (PNR), aangezien het gecombineerde gebruik van PNR- en API-gegevens de doeltreffendheid van PNR-gegevens verder verbetert in de bestrijding van terrorisme en zware criminaliteit[19].

Visuminformatiesysteem (VIS)

De Commissie is ook bezig met een algemene evaluatie van het **Visuminformatiesysteem** (VIS), die in 2016 moet worden afgerond. De evaluatie heeft onder meer betrekking op de wijze waarop het VIS wordt gebruikt voor controles aan de buitengrenzen en op het grondgebied van de lidstaten, en de wijze waarop het bijdraagt tot de bestrijding van identiteits- en visumfraude. Op basis van de resultaten daarvan zal de Commissie vervolgens de mogelijkheden onderzoeken om de functies van het VIS te verbeteren, onder meer door:

- de kwaliteit van gezichtsopnamen te verbeteren om biometrische matching mogelijk te maken;
- de biometrische gegevens van visumaanvragers te gebruiken om te zoeken in het toekomstige geautomatiseerde systeem voor de identificatie van vingerafdrukken, dat voor het SIS moet worden ontwikkeld;
- de leeftijdsgrens voor het afnemen van vingerafdrukken van kinderen tussen 6 en 12 jaar oud te verlagen en tegelijkertijd te voorzien in robuuste waarborgen in het kader van de grondrechten en in beschermingsmaatregelen[20];
- het raadplegen van de Interpol-gegevensbank (SLTD) bij een visumaanvraag te vergemakkelijken.

De mogelijkheden om in het huidige rechtskader toegang te krijgen tot VIS-gegevens voor **rechtshandhavingsdoeleinden**, worden door de lidstaten op ongelijke wijze toegepast. In dit verband hebben de lidstaten praktische problemen gemeld bij de procedures voor toegang tot het VIS door rechtshandhavingsinstanties. Evenzo is de implementatie van de toegang tot Eurodac voor rechtshandhavingsdoeleinden nog steeds zeer beperkt. De Commissie zal onderzoeken of het nodig is om het rechtskader voor toegang tot het VIS en Eurodac voor rechtshandhavingsdoeleinden te herzien.

Eurodac

Zoals uiteengezet in de mededeling "Naar een hervorming van het gemeenschappelijk asielstelsel en een verbetering van de legale mogelijkheden om naar Europa te komen"[21], zal de Commissie een voorstel indienen voor de hervorming van **Eurodac** teneinde de functies ervan verder te verbeteren wat betreft irreguliere migratie en terugkeer. Hiermee zal worden tegemoetgekomen aan een bestaande lacune in het vermogen om secundaire stromen van irreguliere migranten tussen lidstaten op te sporen. Het voorstel zal er bovendien naar streven de doeltreffendheid van terugkeer- en overnameprocedures te verbeteren door te voorzien in middelen om irreguliere migranten voor terugkeerdoeleinden te identificeren en opnieuw van documenten te voorzien. In dit verband zal het voorstel ook betrekking hebben op uitwisseling van Eurodac-gegevens met derde landen, met inachtneming van de nodige waarborgen inzake gegevensbescherming.

---

[19] Zie punt 6.2 over de voorgestelde PNR-richtlijn.

[20] Zoals aangegeven als technisch haalbaar in de JRC-studie "Fingerprint Recognition for children"; EUR 26193 EN; ISBN 978-92-79-33390-3Children', 2013.

[21] COM(2016)197 final.

Europol

De EU heeft **Europol** toegang verleend tot de belangrijkste centrale gegevensbanken, maar het agentschap heeft nog niet ten volle gebruik gemaakt van deze mogelijkheid. Europol heeft recht op toegang tot het SIS en het recht om rechtstreeks te zoeken naar gegevens die in het SIS zijn opgenomen met het oog op aanhouding, onopvallende en gerichte controles en inbeslagneming. Europol heeft tot dusver slechts een relatief beperkt aantal zoekopdrachten in SIS uitgevoerd. Toegang tot het VIS voor raadpleging is voor Europol wettelijk mogelijk sinds september 2013. Sinds juli 2015 maakt de rechtsgrondslag van Eurodac toegang voor Europol mogelijk. Het agentschap zou meer vaart moeten zetten achter de lopende werkzaamheden om verbinding te maken met het VIS en Eurodac. Meer in het algemeen zal de Commissie nagaan of het nodig is om ook andere EU-agentschappen op het gebied van binnenlandse zaken toegang te verlenen tot informatiesystemen, met name de toekomstige Europese grens- en kustwacht.

Kader van Prüm

Het potentieel van het **kader van Prüm** wordt momenteel nog niet volledig benut. Niet alle lidstaten zijn immers hun wettelijke verplichtingen nagekomen op het gebied van de integratie van hun eigen systemen in het netwerk. De lidstaten hebben aanzienlijke financiële en technische steun ontvangen voor de uitvoering ervan en zouden het kader van Prüm nu volledig moeten implementeren. De Commissie maakt gebruik van de bevoegdheden die haar zijn toegewezen om ervoor te zorgen dat de lidstaten hun wettelijke verplichtingen ten volle uitvoeren, en is in januari 2016 begonnen met een gestructureerde dialoog (EU Pilot) met de betrokken lidstaten. Indien de reacties van de lidstaten niet bevredigend blijken, zal de Commissie niet aarzelen om inbreukprocedures in te leiden.

Europees Strafregister Informatiesysteem (ECRIS)

Met het Europees Strafregister Informatiesysteem **ECRIS** kan informatie worden uitgewisseld over veroordelingen van onderdanen van derde landen en staatlozen, maar er is geen procedure om dat efficiënt te doen. In januari 2016 heeft de Commissie een wetgevingsvoorstel aangenomen om deze lacune aan te pakken[22]. In dit verband heeft de Commissie voorgesteld om het voor de nationale autoriteiten mogelijk te maken om op basis van vingerafdrukken te zoeken naar onderdanen van derde landen met het oog op een veiliger identificatie. Het Europees Parlement en de Raad zullen deze wetgeving naar verwachting in 2016 goedkeuren.

Horizontale kwesties

Een algemeen punt van zorg in verband met informatiesystemen is de **mate van tenuitvoerlegging** door de lidstaten. De ongelijke uitvoering van het kader van Prüm en de ontbrekende elektronische verbindingen met de SLTD-gegevensbank zijn hiervan treffende voorbeelden. Om het tenuitvoerleggingsniveau op het gebied van informatiesystemen te verhogen, zal de Commissie nauwlettend toezien op de prestaties van iedere lidstaat[23]. Bij dat toezicht zal niet alleen worden nagegaan of de lidstaten hun wettelijke verplichtingen op het gebied van informatiesystemen nakomen, maar ook hoe zij gebruikmaken van bestaande instrumenten en of beste praktijken worden nagevolgd. De Commissie zal gebruikmaken van verschillende bronnen bij het controleren en bevorderen van het tenuitvoerleggingsniveau, met inbegrip van de kennisgevingen van de

[22] COM(2016) 7 final van 19.1.2016.

[23] Behoudens de bijzondere bepalingen van protocol nr. 22 wat Denemarken betreft en de protocollen nrs. 21 en 36 wat het Verenigd Koninkrijk en Ierland betreft.

lidstaten en de bezoeken in het kader van het Schengenevaluatie- en -toezichtmechanisme.

Een ander punt van zorg in verband met informatiesystemen is de **kwaliteit van de ingevoerde gegevens**. Indien de lidstaten niet voldoen aan minimumeisen inzake kwaliteit, worden de betrouwbaarheid en de waarde van de opgeslagen gegevens zeer beperkt en ondermijnt het risico van mismatches en niet-treffers de waarde van de systemen zelf. Om de kwaliteit van de ingevoerde gegevens te verbeteren, zal eu-LISA een **centrale controlecapaciteit voor gegevenskwaliteit** ontwikkelen voor alle systemen die onder haar bevoegdheid vallen.

De meeste informatiesystemen op het gebied van grenstoezicht en veiligheid bevatten gegevens die afkomstig zijn uit reis- en identiteitsdocumenten. Voor een beter grenstoezicht en meer veiligheid moeten, naast goed-presterende systemen, reis- en identiteitsdocumenten gemakkelijk en veilig kunnen worden geauthenticeerd. Te dien einde zal de Commissie maatregelen voorstellen ter verbetering van de elektronische **documentbeveiliging** en ID-beheer en ter versterking van de bestrijding van documentenfraude. De interoperable niveaus van veilige identificatie die via de eIDAS-verordening kunnen worden bereikt[24], zouden daarvoor een middel kunnen zijn.

Maatregelen om de bestaande informatiesystemen te verbeteren

Schengeninformatiesysteem (SIS)

- De Commissie en eu-LISA ontwikkelen en implementeren een geautomatiseerd identificatiesysteem voor vingerafdrukken (AFIS) als functionaliteit in het SIS tegen medio 2017.
- De Commissie dient uiterlijk eind 2016 voorstellen in tot herziening van de rechtsgrondslag van het SIS om de functies verder te verbeteren.
- De lidstaten maken zoveel mogelijk gebruik van het SIS, zowel door alle relevante informatie in te voeren als door het systeem te raadplegen telkens wanneer dat nodig is.

De Interpol-gegevensbank voor gestolen en verloren reisdocumenten (SLTD)

- De lidstaten leggen elektronische verbindingen met Interpol-instrumenten op al hun grensdoorlaatposten aan de buitengrenzen.
- De lidstaten komen hun verplichting na om tegelijkertijd in het SIS en in de SLTD-gegevensbank gegevens over gestolen of verloren reisdocumenten in te voeren en te raadplegen.

Advance Passenger Information (API)

- De lidstaten automatiseren het gebruik van API-gegevens voor controles aan de hand van het SIS en de Interpol-gegevensbank voor verloren en gestolen reisdocumenten (SLTD), overeenkomstig de bestaande beste praktijk.
- De Commissie onderzoekt de noodzaak om de rechtsgrondslag voor de verwerking van API-gegevens te herzien.

[24] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG

Visuminformatiesysteem (VIS)

- De Commissie onderzoekt vóór eind 2016 of het VIS verder kan worden verbeterd.

Eurodac

- De Commissie dient een voorstel in om de rechtsgrondslag van Eurodac te herzien, om de functies ervan op het gebied van irreguliere migratie en terugkeer nog te verbeteren.

Europol

- Europol maakt ten volle gebruik van haar bestaande toegangsrechten voor raadpleging van SIS, VIS en Eurodac.
- De Commissie en Europol gaan op zoek naar synergieën tussen het Europol-informatiesysteem (EIS) en andere systemen, met name het SIS, en deze bevorderen.
- De Commissie en eu-LISA gaan na of het geautomatiseerd identificatiesysteem voor vingerafdrukken (AFIS) dat voor het SIS moet worden ontwikkeld, de Europol-systemen voor strafrechtelijk onderzoek en bestrijding van terrorisme kan aanvullen.

Kader van Prüm

- De lidstaten leggen het kader van Prüm volledig ten uitvoer en maken er volledig gebruik van.
- Indien nodig leidt de Commissie inbreukprocedures in tegen lidstaten die nog niet met het kader van Prüm zijn verbonden.
- De Commissie en eu-LISA gaan na of het geautomatiseerd identificatiesysteem voor vingerafdrukken (AFIS) dat voor het SIS moet worden ontwikkeld, de uitwisseling van vingerafdrukken in het kader van Prüm kan aanvullen.

Europees Strafregister Informatiesysteem (ECRIS)

- Het Europees Parlement en de Raad zouden in 2016 het wetgevingsvoorstel moeten goedkeuren om de nationale autoriteiten in staat te stellen op basis van vingerafdrukken in ECRIS te zoeken naar onderdanen van derde landen.

Horizontale kwesties

- De Commissie **houdt toezicht op en bevordert het niveau van tenuitvoerlegging** op het gebied van informatiesystemen.
- eu-LISA ontwikkelt een **centrale controlecapaciteit voor gegevenskwaliteit** voor alle systemen die onder haar bevoegdheid vallen.
- De Commissie stelt maatregelen voor ter verbetering van de elektronische **documentbeveiliging en ID-beheer** en ter versterking van de bestrijding van documentenfraude.
- De Commissie zoekt naar synergieën en convergentie tussen informatiesystemen en de bijbehorende infrastructuur ten behoeve van het EU-grensbeheer en **douaneverrichingen**.

6. ONTWIKKELEN VAN AANVULLENDE INFORMATIESYSTEMEN EN AANPAKKEN VAN LACUNES

De bestaande informatiesystemen dekken weliswaar een zeer breed spectrum van gegevens, hetgeen vereist is in het kader van grensbeheer en rechtshandhaving, maar er zijn belangrijke lacunes. Sommige daarvan zijn door de Commissie aangepakt met wetgevingsvoorstellen, namelijk de voorstellen voor een inreis-uitreissysteem en voor een EU-regeling voor persoonsgegevens van passagiers (PNR). Voor andere vastgestelde

lacunes moet grondig worden nagegaan of aanvullende EU-instrumenten noodzakelijk zijn.

1. Inreis-uitreissysteem

De Commissie heeft samen met deze mededeling het herziene wetgevingsvoorstel voor de instelling van een inreis-uitreissysteem (EES) voorgesteld. Na de goedkeuring ervan door de medewetgevers zal eu-LISA het systeem moeten ontwikkelen en ten uitvoer leggen in samenwerking met de Schengenlidstaten.

In het EES zullen de grensoverschrijdingen (inreis en uitreis) van derdelanders worden geregistreerd die het Schengengebied bezoeken voor een kort verblijf (ten hoogste 90 dagen binnen een periode van 180 dagen), ongeacht of deze reizigers visumplichtig of niet-visumplichtig zijn, en voor verblijf op basis van het nieuwe rondreisvisum (maximale geldigheidsduur één jaar). Het EES heeft als doel a) het beheer van de buitengrenzen te verbeteren, b) irreguliere migratie te beperken, door het fenomeen aan te pakken van het langer verblijven dan toegestaan en c) bij te dragen tot de bestrijding van terrorisme en zware misdaad, en zo ook bij te dragen tot het waarborgen van een hoog niveau van interne veiligheid.

In het EES wordt de identiteit van onderdanen van derde landen geregistreerd (alfanumerieke gegevens, vingerafdrukken en gezichtsopname), samen met gedetailleerde gegevens van hun reisdocumenten, en worden deze verbonden met de elektronische inreis- en uitreisgegevens. De huidige praktijk van het stempelen van reisdocumenten zal worden stopgezet. Het EES zal doeltreffend beheer van toegestane korte verblijven mogelijk maken, zorgen voor sterkere automatisering van de grenscontroles en de opsporing van documenten- en identiteitsfraude verbeteren. De centrale registratie zal het mogelijk maken om vast te stellen of er langer wordt verbleven dan toegestaan en om personen zonder papieren in het Schengengebied te identificeren. Met het voorgestelde EES wordt derhalve een belangrijke lacune in het landschap van bestaande informatiesystemen aangepakt.

2. Passenger Name Records

Passenger Name Record (PNR) gegevens zijn boekingsgegevens, zoals contactgegevens, alle reis- en reservatiegegevens, bijzondere opmerkingen, zitplaats- en bagage-informatie en betaalmiddelen. PNR-gegevens zijn nuttig en noodzakelijk om vast te stellen welke reizigers een hoog risico vormen in het kader van de bestrijding van terrorisme, drugshandel, mensenhandel, seksuele uitbuiting van kinderen, en andere ernstige criminaliteit. De voorgestelde richtlijn inzake PNR-gegevens zal een betere samenwerking tussen de nationale stelsels mogelijk maken en zal de verschillen tussen de lidstaten op het gebied van veiligheid kleiner maken. Met de voorgestelde PNR-richtlijn wordt derhalve een belangrijke lacune in de beschikbaarheid van gegevens aangepakt die noodzakelijk is voor de bestrijding van ernstige criminaliteit en terrorisme. **De PNR-richtlijn zou onverwijld moeten worden aangenomen en uitgevoerd.**

De toekomstige richtlijn zal bepalen dat de lidstaten passagiersinformatie-eenheden (PIU) moeten oprichten die PNR-gegevens zullen ontvangen van luchtvaartmaatschappijen. Dit zal niet leiden tot de oprichting van een centraal systeem of centrale gegevensbank, maar een meerwaarde hebben in de zin van een bepaalde mate van standaardisering van nationale technische oplossingen en procedures. Op die manier zal de uitwisseling van PNR-gegevens tussen de PIU's worden vergemakkelijkt, zoals in de richtlijn bepaald. Daartoe zal de Commissie de lidstaten helpen bij het analyseren van verschillende scenario’s voor de interconnectie tussen PIU's, met het oog op het aanbieden van gestandaardiseerde oplossingen en procedures. Zodra de richtlijn is

aangenomen, zal de Commissie meer vaart zet achter de werkzaamheden inzake gemeenschappelijke protocollen en ondersteunde dataformaten voor het doorgeven van PNR-gegevens door luchtvaartmaatschappijen aan de PIU's. De Commissie zal een ontwerpuitvoeringshandeling vaststellen binnen drie maanden na de aanneming van de richtlijn.

3. Gebrek aan informatie vóór de aankomst van niet-visumplichtige onderdanen van derde landen

Terwijl de identiteit, contacten en achtergrondinformatie van visumhouders in het VIS zijn geregistreerd, is de enige informatie over niet-visumplichtige personen afkomstig van hun reisdocument. Voor reizigers die per vliegtuig of over zee reizen, komen daar mogelijk ook API-gegevens vóór aankomst bij. Op grond van de voorgestelde PNR-richtlijn zullen hun PNR-gegevens ook worden verzameld indien zij per vliegtuig in de EU aankomen. Voor personen die via de landgrenzen de EU binnenkomen, is aan de buitengrenzen van de EU geen informatie beschikbaar vóór hun aankomst.

Terwijl rechtshandhavingsinstanties informatie over visumhouders kunnen krijgen uit het VIS indien dit noodzakelijk is voor de bestrijding van zware criminaliteit en terrorisme, zijn er geen vergelijkbare gegevens beschikbaar over niet-visumplichtige personen. Dit gebrek aan informatie is vooral relevant voor het beheer van de landgrenzen van de EU, in een situatie waarin grote aantallen niet-visumplichtige reizigers aankomen per auto, bus of trein. Verschillende buurlanden van de EU zijn reeds van de visumplicht vrijgesteld en tussen de EU en andere buurlanden worden dialogen over visumliberalisering gevoerd. Dit zal waarschijnlijk leiden tot een aanzienlijke toename van niet-visumplichtige reizigers in de nabije toekomst.

De Commissie zal nagaan of een nieuw EU-instrument om dit probleem aan te pakken, nodig, haalbaar en proportioneel is. Een optie die kan worden overwogen, is een **EU-Systeem voor reisinformatie en -autorisatie** (ETIAS) waarin niet-visumplichtige reizigers informatie kunnen registreren over hun voorgenomen reis. De automatische verwerking van deze informatie zou grenswachten kunnen helpen bij hun onderzoek van bezoekers uit derde landen die binnenkomen voor een kort verblijf. Landen als de VS, Canada en Australië hebben reeds soortgelijke systemen opgezet, onder meer voor EU-burgers.

Systemen voor reisautorisatie zijn gebaseerd op online-aanvragen waarbij de aanvrager vóór vertrek details verstrekt over zijn/haar identiteit, contactgegevens, doel van de reis, reisroute, enz. Zodra de autorisatie is verkregen, verlopen de grensprocedures bij aankomst sneller en vlotter. Naast de voordelen voor de veiligheid en het grensbeheer, en het potentiële belang in het kader van visumwederkerigheid, zou een systeem als ETIAS derhalve ook dienen als een instrument dat reizen gemakkelijker maakt.

4. Europees informatiesysteem voor politiegegevens (EPRIS)

Zoals aangegeven in de Europese veiligheidsagenda is de realtimebeschikbaarheid van bestaande politiegegevens voor de lidstaten een gebied voor toekomstige werkzaamheden inzake informatie-uitwisseling. De Commissie zal de noodzaak, de technische haalbaarheid en de evenredigheid onderzoeken van een Europees indexsysteem voor politiegegevens (EPRIS) om de grensoverschrijdende toegang tot informatie in nationale gegevensbanken voor rechtshandhaving te vergemakkelijken. In dit verband steunt de Commissie met EU-financiering de uitvoering van een proefproject door een groep van vijf lidstaten om een mechanisme in te stellen voor geautomatiseerde grensoverschrijdende opzoekingen in nationale registers op basis een "treffer/geen

treffer" -systeem[25]. De Commissie zal bij haar onderzoek rekening houden met de resultaten van dat project.

Maatregelen om aanvullende informatiesystemen te ontwikkelen en lacunes op het gebied van informatie aan te pakken

Inreis-uitreissysteem (EES)

- Het Europees Parlement en de Raad zouden de wetgevingsvoorstellen over het EES met de hoogste prioriteit moeten behandelen, zodat deze tegen eind 2016 kunnen worden aangenomen.

Passenger Name Records (PNR)

- Het Europees Parlement en de Raad zouden de richtlijn inzake PNR-gegevens tegen april 2016 moeten goedkeuren.
- Zodra de richtlijn over PNR-gegevens is goedgekeurd, geven de lidstaten daaraan onverwijld uitvoering.
- De Commissie zal de uitwisseling van gegevens tussen de passagiersinformatie-eenheden steunen door middel van gestandaardiseerde oplossingen en procedures.
- De Commissie bereidt binnen drie maanden na de goedkeuring van de PNR-richtlijn een ontwerpuitvoeringshandeling voor over gemeenschappelijke protocollen en ondersteunde dataformaten voor het doorgeven van PNR-gegevens door luchtvaartmaatschappijen aan de passagiersinformatie-eenheden.

Gebrek aan informatie vóór de aankomst over niet-visumplichtige onderdanen van derde landen

- De Commissie gaat in 2016 na of het noodzakelijk, technisch haalbaar en evenredig is om een nieuw EU-instrument op te zetten, zoals een EU-Systeem voor reisinformatie en -autorisatie.

Europees informatiesysteem voor politiegegevens (EPRIS)

- De Commissie gaat in 2016 na of het noodzakelijk, technisch haalbaar en evenredig is om een EPRIS op te zetten.

7. NAAR INTEROPERABILITEIT VAN INFORMATIESYSTEMEN

Interoperabiliteit is het vermogen van informatiesystemen om onderling gegevens uit te wisselen en het delen van informatie mogelijk te maken. Er kan een onderscheid worden gemaakt tussen **vier dimensies van interoperabiliteit,** die elk juridische[26], technische en operationele vragen oproepen, onder meer inzake gegevensbescherming:

- één enkele zoekinterface om gelijktijdig verschillende informatiesystemen te raadplegen, leidend tot gecombineerde zoekresultaten op één enkel scherm;

[25] Het proefproject voor de procedure voor geautomatiseerde gegevensuitwisseling (ADEP) beoogt het opzetten van een technisch systeem waarmee via een index kan worden nagegaan of er in een of meerdere lidstaten politiegegevens bestaan over een individu of een politieel strafonderzoek. Het geautomatiseerde antwoord op een zoekopdracht in de index zou alleen aangeven of er al dan niet gegevens beschikbaar zijn; een zogenaamd "treffer" of "geen treffer" antwoord. In het geval van een "treffer" zouden dan in een tweede stap aanvullende persoonsgegevens moeten worden opgevraagd via de gebruikelijke kanalen voor politiële samenwerking.

[26] Behoudens de bijzondere bepalingen van protocol nr. 22 wat Denemarken betreft en de protocollen nrs. 21 en 36 wat het Verenigd Koninkrijk en Ierland betreft.

- de interconnectiviteit van informatiesystemen waardoor in het ene systeem geregistreerde gegevens automatisch worden geraadpleegd via een ander systeem;
- de oprichting van een gezamenlijke dienst voor biometrische matching ter ondersteuning van verschillende informatiesystemen;
- een gemeenschappelijk gegevensregister voor verschillende informatiesystemen (kernmodule).

Om de aanzet te geven voor een proces dat moet leiden tot de interoperabiliteit van informatiesystemen op EU-niveau, zal de Commissie een **deskundigengroep inzake informatiesystemen en interoperabiliteit** op hoog niveau oprichten, met EU-instanties, nationale deskundigen en betrokken institutionele belanghebbenden. De deskundigengroep zal worden belast met de juridische, technische en operationele aspecten van de verschillende opties om te komen tot de interoperabiliteit van informatiesystemen, met inbegrip van de noodzaak, de technische haalbaarheid en de evenredigheid van de beschikbare opties en de gevolgen ervan voor de gegevensbescherming. Zij moet de huidige tekortkomingen en lacunes in de kennis behandelen die worden veroorzaakt door de complexiteit en versnippering van de informatiesystemen op Europees niveau. De deskundigengroep zal werken met een brede en alomvattende kijk op grensbeheer en rechtshandhaving, waarbij tevens rekening wordt gehouden met de rol, de bevoegdheden en de systemen van douaneautoriteiten op dit gebied. De werkmethode van de groep zal als doel hebben alle relevante ervaring samen te brengen, die in het verleden te vaak afzonderlijk werd ontwikkeld.

Dit proces heeft als doel een algemene strategische visie te ontwikkelen op de EU-architectuur voor gegevensbeheer voor grenstoezicht en veiligheid, alsmede om oplossingen te vinden voor de tenuitvoerlegging ervan.

Bij deze overlegprocedure zullen **de volgende doelstellingen** leidend zijn:

- De informatiesystemen moeten complementair zijn. Overlappingen moeten worden vermeden, en bestaande overlappingen moeten worden weggewerkt. Lacunes moeten op passende wijze worden aangepakt.
- Er moet sprake zijn van een modulaire aanpak, waarbij ten volle gebruik wordt gemaakt van technologische ontwikkelingen en de beginselen van "ingebouwde privacy" worden gevolgd.
- Van meet af aan moeten alle grondrechten van zowel EU-burgers als onderdanen van derde landen ten volle worden gewaarborgd overeenkomstig het Handvest van de grondrechten.
- Als dat noodzakelijk en haalbaar is, moeten informatiesystemen onderling worden verbonden en interoperabel zijn. Gelijktijdig zoeken in systemen moet worden vergemakkelijkt, zodat alle relevante informatie beschikbaar is voor grenswachten of politiefunctionarissen waar en wanneer dat nodig is voor het vervullen van hun respectieve taken, zonder de bestaande toegangsrechten te wijzigen.

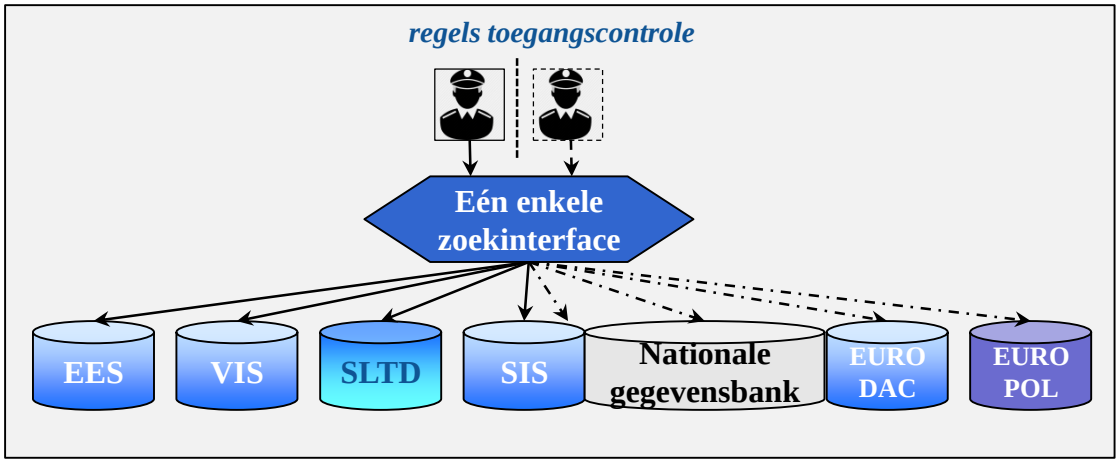
1. Een enkele zoekinterface

De eerste dimensie van interoperabiliteit is de mogelijkheid voor grenswachten en politiefunctionarissen **om gelijktijdig verschillende informatiesystemen te raadplegen, leidend tot gecombineerde zoekresultaten op één enkel scherm**, met volledige inachtneming van hun toegangsrechten, in overeenstemming met de respectieve doeleinden. Dit vergt platforms met één enkele zoekinterface die met één enkele zoekopdracht in staat zijn gelijktijdig informatiesystemen te raadplegen. Dat platform zou bijvoorbeeld door het uitlezen van de chip van een reisdocument of door

gebruik te maken van biometrische gegevens, verschillende gegevensbanken tegelijk kunnen raadplegen. De één-zoekopdracht-benadering geldt voor alle autoriteiten die toegang tot de gegevens moeten kunnen hebben en daarvan gebruik moeten kunnen maken (d.w.z. grenswachten, rechtshandhavingsinstanties, asieldiensten), overeenkomstig het beginsel van de doelbeperking en de strikte regels inzake toegangscontrole. Zij kan ook met mobiele apparatuur worden toegepast. Het instellen van één enkele zoekinterface vermindert de complexiteit van informatiesystemen op Europees niveau, aangezien het grenswachten en politiefunctionarissen in staat stelt gelijktijdig verschillende informatiesystemen te raadplegen via één procedure en in overeenstemming met hun toegangsrechten.

Verscheidene lidstaten hebben reeds dergelijke platforms met één enkele zoekinterface ingesteld. Op basis van deze bestaande beste praktijken zal de Commissie samen met eu-LISA werken aan de ontwikkeling van een gestandaardiseerde oplossing voor één enkele zoekinterface. De lidstaten moeten gebruikmaken van EU-financiering in het kader van hun nationale programma voor het Fonds voor interne veiligheid ter financiering van de installatie van een dergelijke functionaliteit. De Commissie zal nauwlettend toezien op de wijze waarop de lidstaten gebruikmaken van de functionaliteit van één enkele zoekinterface op nationaal niveau.

Figuur 2 *Een enkele zoekinterface*



Zoeken in meerdere gecentraliseerde of nationale systemen (zoals afgebeeld) is gemakkelijker te realiseren dan zoeken in gedecentraliseerde systemen. De Commissie en eu-LISA zullen nagaan of één enkele zoekinterface ook kan worden gebruikt om gelijktijdig "aan één loket" te zoeken in gedecentraliseerde systemen zoals Prüm en ECRIS. De Commissie en eu-LISA zullen deze analyse maken samen met de deskundigengroep inzake informatiesystemen en interoperabiliteit, zonder wijziging van de bestaande toegangsrechten.

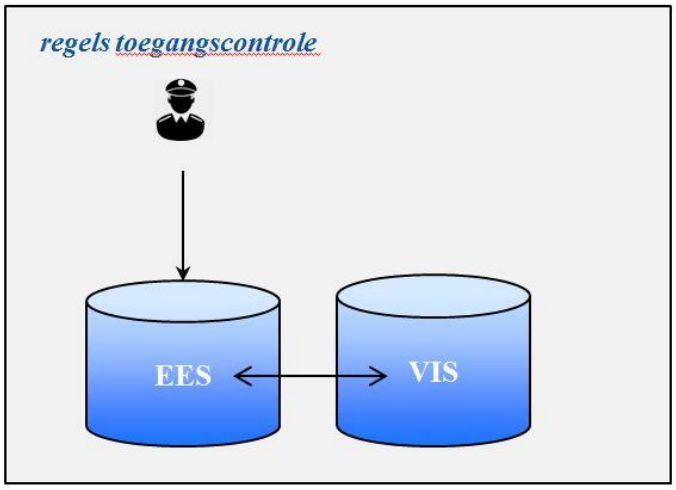
2. Interconnectiviteit van informatiesystemen

Een tweede dimensie van interoperabiliteit is de interconnectiviteit van informatiesystemen. Dit betekent dat verschillende systemen of gegevensbanken technisch gezien "met elkaar kunnen communiceren". **Gegevens die in één systeem zijn geregistreerd, zouden automatisch op centraal niveau door een ander systeem kunnen worden geraadpleegd.** Dit vereist dat de systemen technisch compatibel zijn en dat de in deze systemen opgeslagen gegevens (zoals vingerafdrukken) interoperabel zijn. Interconnectiviteit kan de hoeveelheid gegevens die binnen de communicatienetwerken circuleren en via nationale systemen lopen, beperken.

Interconnectiviteit vereist passende garanties op het gebied van gegevensbescherming en strikte regels inzake toegangscontrole. Het in december 2015 door de medewetgevers bereikte politieke akkoord over de hervorming van de gegevensbescherming zal zorgen voor een modern kader inzake gegevensbescherming voor de hele EU dat in deze waarborgen zal voorzien. Het is belangrijk dat de medewetgevers onverwijld de algemene verordening over gegevensbescherming en de richtlijn over gegevensbescherming aannemen.

Het concept interconnectiviteit is ingebouwd in het toekomstige EES. Het toekomstige EES zal rechtstreeks kunnen communiceren met het VIS op centraal niveau en vice versa. Dit is een belangrijke stap in de aanpak van de huidige fragmentatie van de EU-architectuur voor gegevensbeheer voor grenstoezicht en veiligheid, en van de daarmee verband houdende problemen. De geautomatiseerde kruiscontrole zal de lidstaten ontslaan van de noodzaak om het VIS te raadplegen bij grenscontroles, zorgen voor minder onderhoudsvoorschriften en de prestaties van het systeem verbeteren.

Figure 3 *Interconnectiviteit van systemen: het voorbeeld van EES/VIS*



Als volgende stap zullen de Commissie en eu-LISA nagaan of de interconnectiviteit op centraal niveau tussen het toekomstige EES en het VIS kan worden uitgebreid tot het SIS en of interconnectiviteit tussen Eurodac en het SIS mogelijk is. De Commissie en eu-LISA zullen deze analyse maken samen met de deskundigengroep inzake informatiesystemen en interoperabiliteit.

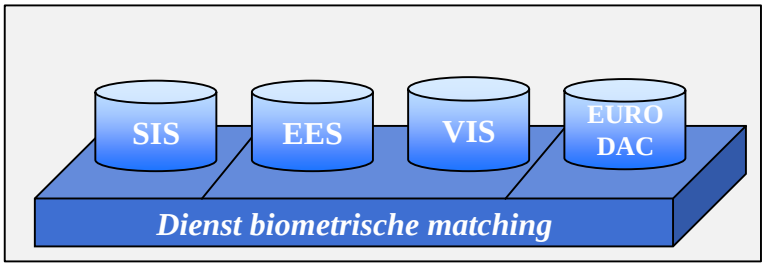
3. Gemeenschappelijke dienst voor biometrische matching

Een derde dimensie van interoperabiliteit heeft betrekking op biometrische identificatiemiddelen. Wanneer bijvoorbeeld op een consulaat van een lidstaat met specifieke apparatuur vingerafdrukken worden afgenomen, is het van cruciaal belang dat er voor deze afdrukken via het VIS een match mogelijk is aan een grenspost van een andere lidstaat, waar een ander type apparatuur wordt gebruikt. Hetzelfde geldt voor zoekopdrachten naar vingerafdrukken in andere systemen: biometrische monsters moeten voldoen aan minimumeisen inzake kwaliteit en vorm, wil dit soort interoperabiliteit zonder problemen mogelijk zijn.

Op het niveau van het systeem maakt de interoperabiliteit van biometrische identificatiemiddelen het mogelijk gebruik te maken van een gemeenschappelijke dienst voor biometrische matching voor verschillende informatiesystemen, met inachtneming van de regels inzake de bescherming van persoonsgegevens door de gegevens te

compartimenteren, met afzonderlijke regels inzake toegangscontrole voor elke gegevenscategorie[27]. Dergelijke gemeenschappelijke diensten leveren ernstige financiële en operationele voordelen op, alsook voordelen op het vlak van onderhoud.

Figuure 4 *Gemeenschappelijke dienst voor biometrische matching*



De Commissie en eu-LISA zullen nagaan of de oprichting van een gemeenschappelijke dienst voor biometrische matching voor alle relevante informatiesystemen nodig en technisch haalbaar is. De Commissie en eu-LISA zullen deze analyse maken samen met de deskundigengroep inzake informatiesystemen en interoperabiliteit.

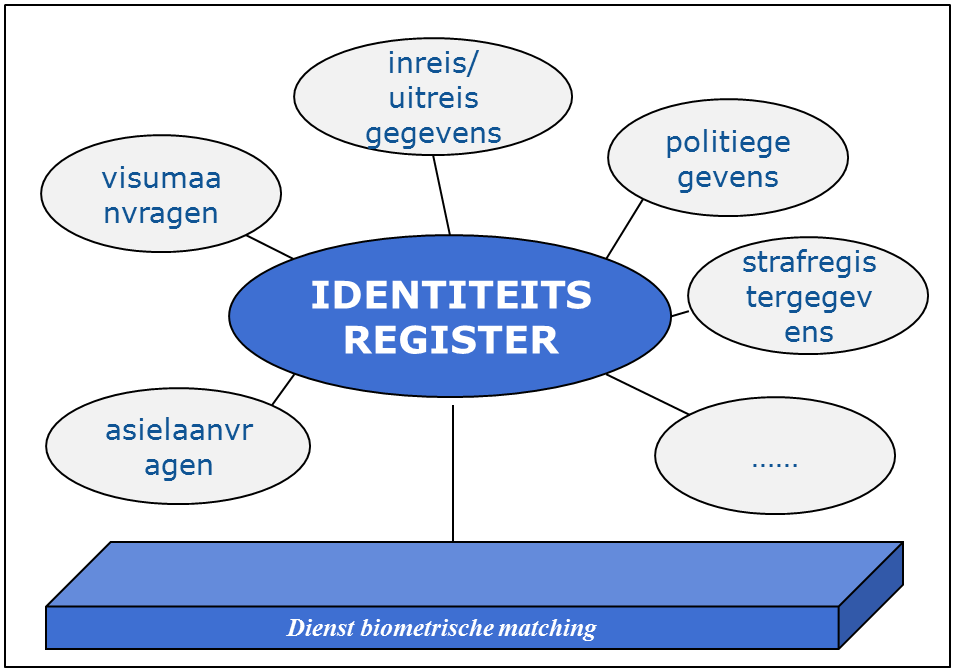
4. Gemeenschappelijk gegevensregister

De meest ambitieuze langetermijnvisie op interoperabiliteit is een **gemeenschappelijk register van gegevens op EU-niveau voor verschillende informatiesystemen**. Het gemeenschappelijke gegevensregister zou bestaan uit een kernmodule die de basisgegevens bevat (alfanumerieke en biometrische gegevens), terwijl andere gegevenselementen en specifieke kenmerken van de diverse informatiesystemen (bv. visumgegevens) in specifieke modules zouden worden opgeslagen. De kernmodule en de specifieke modules zouden aan elkaar worden gekoppeld om de respectieve gegevensreeksen met elkaar te verbinden. Dit zou leiden tot een **modulair en geïntegreerd identiteitsbeheer voor grenzen en veiligheid**. De naleving van de voorschriften inzake gegevensbescherming zou gegarandeerd moeten worden, bijvoorbeeld door de gegevens te compartimenteren, met afzonderlijke regels inzake toegangscontroles voor elke gegevenscategorie.

Het opzetten van een gemeenschappelijk gegevensregister zou een oplossing vormen voor de huidige fragmentatie van de EU-architectuur voor gegevensbeheer voor grenstoezicht en veiligheid. Deze fragmentatie is in strijd met het beginsel van minimale gegevensverwerking aangezien zij ertoe leidt dat dezelfde gegevens meermaals worden opgeslagen. Indien nodig zou de gemeenschappelijke gegevensbank de erkenning van verbindingen mogelijk maken en een algemeen beeld geven door een combinatie van individuele gegevenselementen die in de verschillende informatiesystemen zijn opgeslagen. Op die manier zou zij de huidige informatielacunes aanpakken en een licht werpen op blinde vlekken voor grenswachten en politiefunctionarissen.

Figuur 5 *Gemeenschappelijk gegevensregister*

[27] Vergelijkbaar met het delen van één fysieke file-server door een groot aantal gebruikers, waarbij elke gebruiker slechts voor bepaalde bestandsmappen specifieke toegangsrechten heeft.



De optie om een gemeenschappelijk gegevensregister op EU-niveau op te richten, doet belangrijke vragen rijzen over het bepalen van het doel, de noodzakelijkheid, de technische haalbaarheid en de evenredigheid van de betrokken gegevensverwerking. Het zou een volledige herziening vereisen van het rechtskader waarbinnen de verschillende informatiesystemen zijn opgezet en zou alleen als doelstelling op de lange termijn kunnen worden bereikt. De deskundigengroep inzake informatiesystemen en interoperabiliteit zal de juridische, technische en operationele kwesties die met een gemeenschappelijk gegevensregister verband houden, behandelen, waaronder ook kwesties inzake gegevensbescherming.

Voor alle vier de hierboven beschreven dimensies van interoperabiliteit (één enkele zoekinterface, interconnectiviteit van systemen, een gemeenschappelijke dienst voor biometrische matching en een gemeenschappelijk gegevensregister) is het noodzakelijk dat de gegevens die in andere informatiesystemen of modules zijn opgeslagen, verenigbaar zijn. Om dit te bereiken, is het van belang dat er werk wordt gemaakt van een **Uniform Message Format** (uniform berichtenformaat, UMF) om een gemeenschappelijke standaard vast te stellen voor alle betrokken informatiesystemen[28].

Maatregelen voor meer interoperabiliteit van informatiesystemen

- De Commissie richt samen met EU-agentschappen, de lidstaten en relevante belanghebbenden een **deskundigengroep inzake informatiesystemen en interoperabiliteit** op om in te gaan op de juridische, technische en operationele aspecten van een grotere interoperabiliteit van informatiesystemen, waaronder de noodzakelijkheid, de technische haalbaarheid en de evenredigheid van de beschikbare opties en de implicaties ervan voor de gegevensbescherming.

[28] De Commissie steunt de verdere ontwikkeling van UMF in de mededeling van 2012 over het Europees model voor informatie-uitwisseling (EIXM) en financiert momenteel het derde UMF proefproject, met als doel een gemeenschappelijke norm vast te stellen voor alle relevante gegevensbanken, die moet worden toegepast op nationaal niveau (lidstaten) op EU-niveau (voor de centrale systemen, en door agentschappen) en op internationaal niveau (Interpol).

Een enkele zoekinterface

- De Commissie en eu-LISA ondersteunen de lidstaten bij de invoering van één enkele zoekinterface om te zoeken in centrale systemen.
- De Commissie en eu-LISA gaan samen met de deskundigengroep na of één enkele zoekinterface zou kunnen worden gebruikt als "één loket" om gelijktijdig zoekopdrachten uit te voeren in alle relevante systemen zonder wijziging van de bestaande toegangsrechten.

Interconnectiviteit van informatiesystemen

- De Commissie en eu-LISA gaan samen met de deskundigengroep na of interconnectiviteit tussen gecentraliseerde informatiesystemen verder kan worden bevorderd, naast de reeds voorgestelde interconnectiviteit tussen het inreis-uitreissysteem en het Visuminformatiesysteem.

Dienst voor biometrische matching

- De Commissie en eu-LISA analyseren samen met de deskundigengroep de noodzakelijkheid en de technische haalbaarheid van het opzetten van een gemeenschappelijke dienst voor biometrische matching voor alle relevante informatiesystemen.

Gemeenschappelijk gegevensregister (kernmodule)

- De Commissie en eu-LISA onderzoeken samen met de deskundigengroep de juridische, technische, operationele en financiële implicaties van de ontwikkeling op langere termijn van een gemeenschappelijk gegevensregister.
- De Commissie en eu-LISA zetten zich in om verder te werken aan een wereldwijd uniform berichtformaat voor alle relevante informatiesystemen.

8. CONCLUSIE

Deze mededeling geeft de aanzet voor een discussie over de vraag hoe informatiesystemen in de EU het grensbeheer en de interne veiligheid beter kunnen bevorderen, voortbouwend op de belangrijke synergieën tussen Europese agenda's voor veiligheid en migratie. Een aantal informatiesystemen levert grenswachten en politiefunctionarissen nu al relevante informatie, maar deze systemen zijn niet volmaakt. De EU wordt geconfronteerd met de uitdaging een sterkere en slimmere architectuur voor gegevensbeheer op te zetten, met volledige inachtneming van de grondrechten, en met name de bescherming van persoonsgegevens en het doelbindingsbeginsel.

Daar waar er sprake is van lacunes in de **EU-architectuur voor gegevensbeheer**, moeten die worden aangepakt. Tegelijk met deze mededeling heeft de Commissie een voorstel ingediend voor een inreis-uitreissysteem dat dringend moet worden goedgekeurd. Ook de richtlijn betreffende Passenger Name Record zou in de komende weken moeten worden goedgekeurd. Het voorstel voor een Europese grens- en kustwacht zou nog voor de zomer moeten zijn aangenomen. Tegelijkertijd zal de Commissie blijven werken aan het versterken en waar nodig het stroomlijnen van de bestaande systemen, zoals het opzetten van een geautomatiseerd identificatiesysteem voor vingerafdrukken als functionaliteit van het Schengeninformatiesysteem.

De lidstaten moeten optimaal gebruik maken van de bestaande informatiesystemen en de noodzakelijke technische verbindingen naar alle informatiesystemen en gegevensbanken tot stand brengen, in overeenstemming met hun wettelijke verplichtingen. Bestaande tekortkomingen, met name in het kader van Prüm, moeten onverwijld worden verholpen.

Terwijl deze mededeling een discussie opent en een proces start om systemische tekortkomingen en gebreken aan te pakken, is het aan de lidstaten om dringend aandacht te besteden aan aanhoudende tekortkomingen inzake het invoeren van gegevens in EU-gegevensbanken en de uitwisseling van informatie in de gehele Unie.

Om de EU-architectuur voor gegevensbeheer voor grenstoezicht en veiligheid structureel te verbeteren, brengt deze mededeling een proces op gang om tot de interoperabiliteit van informatiesystemen te komen. De Commissie zal een deskundigengroep inzake informatiesystemen en interoperabiliteit oprichten ter behandeling van de juridische, technische en operationele voorwaarden van opties voor de verwezenlijking van de interoperabiliteit van informatiesystemen en om lacunes en tekortkomingen aan te pakken. Naar aanleiding van de bevindingen van de deskundigengroep zal de Europese Commissie meer concrete ideeën voorleggen aan het Europees Parlement en de Raad als basis voor gezamenlijk overleg over de verdere gang van zaken. De Commissie zal ook de input vragen van de Europese Toezichthouder voor gegevensbescherming en de nationale gegevensbeschermingsautoriteiten die samenkomen in de Groep artikel 29.

Het doel moet zijn een gezamenlijke strategie te ontwikkelen om het gegevensbeheer in de EU effectiever en efficiënter te maken, met volledige inachtneming van de voorschriften inzake gegevensbescherming, teneinde haar buitengrenzen beter te beschermen en haar interne veiligheid te bevorderen, ten bate van alle burgers.

BIJLAGE 1: AFKORTINGEN

API	Advance Passenger Information (vooraf te verstrekken passagiersgegevens)
AFIS	Automated Fingerprint Identification System (geautomatiseerd systeem voor de identificatie van vingerafdrukken): systeem waarmee vingerafdrukken kunnen worden genomen, opgeslagen, vergeleken en geverifieerd.
CIS	Customs Information System (douane-informatiesysteem)
ECRIS	European Criminal Records Information System (Europees Strafregister Informatiesysteem)
EES	(voorgesteld) Entry-Exit System (inreis-uitreissysteem)
EIXM	European Information Exchange Model (Europees model voor informatie-uitwisseling)
EIS	Europol Information System (Europol-informatiesysteem)
EPRIS	European Police Records Information System (Europees informatiesysteem voor politiegegevens)
EURODAC	European Dactyloscopy (Europees dactyloscopiesysteem)
EUROPOL	European Police Office (Europese Politiedienst), rechtshandhavingsinstantie van de Europese Unie
ETIAS	(mogelijk) EU Travel Information and Authorisation System (EU-Systeem voor reisinformatie en -autorisatie)
eu-LISA	Europees Agentschap voor het operationele beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht.
FIND	Fixed Interpol Networked Database (vaste netwerkgegevensbank van Interpol)
FRONTEX	Europees Agentschap voor het beheer van de operationele samenwerking aan de buitengrenzen van de lidstaten van de Europese Unie
iARMS	Beheersysteem voor het registreren en traceren van illegale vuurwapens (van Interpol)
INTERPOL	International Criminal Police Organization (Internationale Criminele Politie-Organisatie)
MIND	Mobile Interpol Networked Database (mobiele netwerkgegevensbank van Interpol)
PIU	Passenger's Information Unit (passagiersinformatie-eenheid): in elke lidstaat op te richten eenheid om PNR-gegevens te ontvangen van luchtvaartmaatschappijen.
PNR	Passenger Name Record (persoonsgegevens van passagiers)
Prüm	Mechanisme voor politiële samenwerking om informatie uit te wisselen over DNA, vingerafdrukken en gegevens uit kentekenregisters
SafeSeaNet	Europees platform voor de uitwisseling van maritieme gegevens tussen de maritieme autoriteiten van de lidstaten
SBC	Schengen Border Code (Schengengrenscode)
SIENA	Secure Information Exchange Network Application (applicatie van Europol voor veilige informatie-uitwisseling)

SIS	Schengen Information System (Schengeninformatiesysteem, soms aangeduid als van de 2e generatie — SIS II)
SLTD	(Interpol's) Stolen and Lost Travel Documents database (Interpol-gegevensbank voor gestolen en verloren reisdocumenten)
sTESTA	secured Trans European Services for Telematics between Administrations (beveiligde trans-Europese diensten voor telematica tussen overheidsdiensten, te upgraden naar TESTA-NG (volgende generatie))
UMF	Uniform Message Format (uniform berichtformaat): formaat van berichten waardoor informatiesystemen compatibel zijn
VIS	Visa Information System (visuminformatiesysteem)
VRD	Vehicle Registration Data (gegevens uit kentekenregisters)

BIJLAGE 2: OVERZICHT VAN DE BESTAANDE INFORMATIESYSTEMEN VOOR GRENSBEHEER EN RECHTSHANDHAVING

1. Schengeninformatiesysteem (SIS)

Het SIS is het grootste en meest gebruikte platform voor informatie-uitwisseling inzake immigratie en rechtshandhaving. Het is een gecentraliseerd systeem dat door 25 EU-lidstaten[29] en vier met Schengen geassocieerde landen[30] wordt gebruikt en bevat momenteel 63 miljoen signaleringen. Deze worden ingevoerd en geraadpleegd door bevoegde autoriteiten, zoals politie-, grenstoezicht- en immigratiediensten. Het systeem bevat gegevens over onderdanen van derde landen die het Schengengebied niet mogen binnenkomen of er verblijven, alsmede over onderdanen van de EU en van derde landen die gezocht worden of vermist zijn (met inbegrip van kinderen) en over gezochte voorwerpen (vuurwapens, voertuigen, identiteitsdocumenten, industriële uitrusting, enz.). Het onderscheidende kenmerk van SIS in vergelijking met andere instrumenten voor informatie-uitwisseling is dat de informatie wordt aangevuld met een instructie voor concrete actie die functionarissen op het terrein moeten ondernemen, zoals een aanhouding of inbeslagneming.

SIS-controles zijn verplicht voor de verwerking van visa voor kort verblijf, voor grenscontroles voor onderdanen van derde landen en, op niet-systematische basis[31], voor EU-burgers en andere personen die van het recht van vrij verkeer genieten. Bovendien moet elke politiecontrole op het grondgebied ook een automatische controle in SIS omvatten.

2. Visuminformatiesysteem (VIS)

Het VIS is een gecentraliseerd systeem voor de uitwisseling van gegevens over visa voor kort verblijf tussen lidstaten. Het verwerkt gegevens en besluiten met betrekking tot aanvragen voor visa voor kort verblijf om het Schengengebied te bezoeken of erdoor te reizen. Alle consulaten van de Schengenlanden (ongeveer 2000) en al hun doorlaatposten aan de buitengrenzen (in totaal ongeveer 1800) werden met het systeem verbonden.

Het VIS bevat gegevens over visumaanvragen en -besluiten, alsmede informatie over de eventuele intrekking, nietigverklaring of verlenging van afgegeven visa. Het bevat momenteel gegevens over 20 miljoen visumaanvragen en op drukke momenten verwerkt het meer dan 50 000 transacties per uur. Elke visumaanvrager geeft gedetailleerde biografische gegevens, een digitale foto en tien vingerafdrukken. Als zodanig is het een betrouwbare methode om de identiteit van visumaanvragers te controleren, om mogelijke gevallen van irreguliere migratie en veiligheidsrisico's te beoordelen en om "visumshopping" te voorkomen.

Bij grensovergangen of op het grondgebied van de lidstaten wordt het VIS gebruikt om de identiteit van visumhouders te controleren door hun vingerafdrukken te vergelijken met de vingerafdrukken die in het VIS zijn opgeslagen. Zo wordt gegarandeerd dat de persoon die een visum heeft aangevraagd, dezelfde is als degene die de grens overschrijdt. Het zoeken naar vingerafdrukken in het VIS maakt ook de identificatie van

[29] Alle lidstaten, met uitzondering van Cyprus, Ierland en Kroatië.
[30] Zwitserland, Liechtenstein, Noorwegen en IJsland.
[31] Deze regel wordt mogelijk gewijzigd, zoals beoogd in het voorstel van de Commissie (COM/2015/0670) betreffende de wijziging van de Schengengrenscode.

een persoon mogelijk die in de laatste vijf jaar een visum heeft aangevraagd en die eventueel geen identiteitsdocumenten bij zich heeft.

3. Eurodac

Eurodac (Europees dactyloscopiesysteem) bevat de vingerafdrukken van asielzoekers en onderdanen van derde landen die irregulier de buitengrenzen van het Schengengebied overschrijden. Momenteel heeft het als belangrijkste doel te bepalen welke EU-lidstaat verantwoordelijk is voor de behandeling van een asielverzoek, in overeenstemming met de Dublinverordening. Het is beschikbaar aan grensdoorlaatposten, maar anders dan het SIS en het VIS is het geen grensbeheersysteem.

Aan de grensdoorlaatposten worden vingerafdrukken genomen van irreguliere migranten die onrechtmatig de EU binnenkomen. Deze worden opgeslagen in Eurodac om bij een eventueel toekomstig asielverzoek de identiteit van de betrokkene te controleren. Ook immigratie- en politieautoriteiten kunnen vingerafdrukken van irreguliere migranten die in EU-lidstaten worden gevonden, vergelijken om na te gaan of zij in een andere lidstaat asiel hebben aangevraagd. Ook rechtshandhavingsinstanties en Europol hebben het recht om in Eurodac te zoeken om terroristische of andere ernstige delicten te voorkomen, op te sporen of te onderzoeken.

Door vingerafdrukken van asielzoekers of irreguliere migranten in een gecentraliseerd systeem te registreren, kunnen hun secundaire bewegingen[32] binnen de EU worden vastgesteld en gemonitord, totdat een verzoek om internationale bescherming is ingediend of een terugkeerbesluit is genomen (in de toekomst, met een overeenkomstige signalering in het SIS). Meer in het algemeen is het opsporen en monitoren van irreguliere migranten vereist om ervoor te zorgen dat de autoriteiten in hun landen van herkomst hun nieuwe documenten kunnen verstrekken en aldus vergemakkelijkt dit hun terugkeer.

4. De gegevensbank voor gestolen en verloren reisdocumenten (SLTD)

De Interpol-gegevensbank inzake verloren en gestolen reisdocumenten (SLTD) is een centrale gegevensbank voor paspoorten en andere reisdocumenten waarvan de autoriteiten van afgifte aan Interpol hebben gemeld dat zij gestolen of verloren zijn. Zij bevat ook informatie over gestolen blanco paspoorten. Reisdocumenten waarvan aan de autoriteiten van landen die aan het SIS deelnemen, is gemeld dat zij verloren of gestolen zijn, worden zowel in de SLTD als in het SIS opgenomen. De SLTD bevat ook gegevens over reisdocumenten die door landen zijn ingevoerd die niet deelnemen aan het SIS (Ierland, Kroatië, Cyprus en derde landen).

Zoals vermeld in de conclusies van de Raad van 9 en 20 november 2015 en in het voorstel van de Commissie van 15 december 2015 voor een verordening betreffende een gerichte wijziging van de Schengengrenscode[33], zouden de reisdocumenten van alle onderdanen van derde landen en personen die van het recht van vrij verkeer genieten, moeten worden getoetst aan de SLTD. Alle grenscontroleposten moeten met de SLTD worden verbonden. Daar komt nog bij dat binnenlandse zoekopdrachten in de SLTD in het kader van rechtshandhaving extra voordelen opleveren op het gebied van veiligheid.

---

[32] Bijvoorbeeld vluchtelingen die in Griekenland aankomen zonder de bedoeling daar een asielverzoek in te dienen, maar over land naar andere lidstaten willen reizen.

[33] COM(2015) 670 final Voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EG) nr. 562/2006 (EG) inzake het aanscherpen van de controles aan de hand van relevante gegevensbanken aan de buitengrenzen.

5. Advance Passenger Information (API)

API heeft als doel informatie te verzamelen over de identiteit van personen voordat deze aan boord gaan van een inkomende vlucht naar de EU en irreguliere migranten bij aankomst te identificeren. API-gegevens bestaan uit informatie die op reisdocumenten staat en heeft betrekking op de volledige naam, de geboortedatum en de nationaliteit van een reiziger, het nummer en het soort reisdocument, alsook informatie over de grensdoorlaatpost van vertrek en vervoergegevens. Doorgaans worden de API-gegevens van een passagier bij de check-in verzameld.

Krachtens het Verdrag inzake het vergemakkelijken van het internationale verkeer ter zee moet pre-arrival informatie betreffende vervoer over zee 24 uur vóór de geplande aankomst van het vaartuig worden meegedeeld. Richtlijn 2010/65/EU[34] voorziet in elektronische gegevensoverdracht via één loket waarin SafeSeaNet, e-Customs en andere elektronische systemen aan elkaar zijn gekoppeld.

Er is geen centraal EU-systeem voor de registratie van API-gegevens.

6. Europol-informatiesysteem

Het Europol-informatiesysteem (EIS) is een gecentraliseerde gegevensbank met informatie van criminele aard voor onderzoeksdoeleinden. Zij kan worden gebruikt door de lidstaten en Europol om gegevens over zware criminaliteit en terrorisme op te slaan en te raadplegen. In het EIS worden gegevens opgeslagen over personen, identiteitsdocumenten, voertuigen, vuurwapens, telefoonnummers, e-mails, vingerafdrukken, DNA en cybercriminaliteit, die op verschillende manieren aan elkaar kunnen worden gekoppeld teneinde een meer gedetailleerd en gestructureerd beeld van een bepaalde strafzaak te krijgen. Het EIS ondersteunt samenwerking bij rechtshandhaving en is niet beschikbaar voor de grenstoezichtautoriteiten.

De uitwisseling van informatie geschiedt met gebruikmaking van het SIENA[35]-platform, een beveiligd netwerk voor elektronische communicatie tussen Europol, de verbindingsbureaus, en de nationale Europol-eenheden, de aangewezen bevoegde autoriteiten (zoals douane, bureaus voor de ontneming van vermogensbestanddelen, enz.) en de daarmee verbonden derden.

In mei 2017 zal een nieuw rechtskader voor Europol van toepassing worden. Dankzij dit kader zal Europol over een grotere operationele capaciteit beschikken voor analyse en gemakkelijker verbanden kunnen leggen tussen de beschikbare informatie.

7. Kader van Prüm

Het kader van Prüm is gebaseerd op een multilaterale overeenkomst[36] tussen de lidstaten, die het mogelijk maakt DNA-gegevens, vingerafdrukken en gegevens uit kentekenregisters (VRD) uit te wisselen. Het concept is gebaseerd op de interconnectie van een nationaal systeem met de nationale systemen van alle andere EU-lidstaten, zodat cross-searching op afstand mogelijk wordt. Indien een zoekopdracht een positieve match in de gegevensbank van andere lidstaten oplevert, worden de gegevens van die positieve match uitgewisseld met behulp van bilaterale mechanismen voor informatie-uitwisseling.

---

[34] Richtlijn 2010/65/EU van het Europees Parlement en de Raad van 20 oktober 2010 betreffende meldingsformaliteiten voor schepen die aankomen in en/of vertrekken uit havens van de lidstaten en tot intrekking van Richtlijn 2002/6/EG:

[35] Secure Information Exchange Network Application.

[36] Verdrag van Prüm van 2005. Het verdrag is in 2008 in de EU-wetgeving opgenomen door Besluit 2008/615/JBZ van de Raad.

8. Europees Strafregister Informatiesysteem (ECRIS)

ECRIS is een elektronisch systeem voor de uitwisseling van informatie over eerdere veroordelingen van een specifiek persoon door strafrechtbanken in de EU, ten behoeve van een strafrechtelijke procedure tegen een persoon en, indien toegestaan onder de nationale wetgeving, andere doeleinden. Lidstaten waarin een veroordeling wordt uitgesproken jegens een onderdaan van een andere lidstaat, moeten daarvan kennisgeven aan de lidstaat van de nationaliteit van de veroordeelde. De lidstaat van de nationaliteit moet deze informatie bewaren en kan dus op verzoek actuele informatie over de strafrechtelijke veroordelingen van zijn onderdanen verstrekken, ongeacht waar in de EU die zijn uitgesproken.

ECRIS maakt ook de uitwisseling van gegevens over veroordelingen van onderdanen van derde landen en staatlozen mogelijk. In alle lidstaten worden centrale autoriteiten aangewezen als de contactpunten in het ECRIS-netwerk, en zij zijn belast met alle taken, zoals kennisgeving en opslag van gegevens uit strafregisters, en het verzoeken om en verstrekken van dergelijke gegevens.