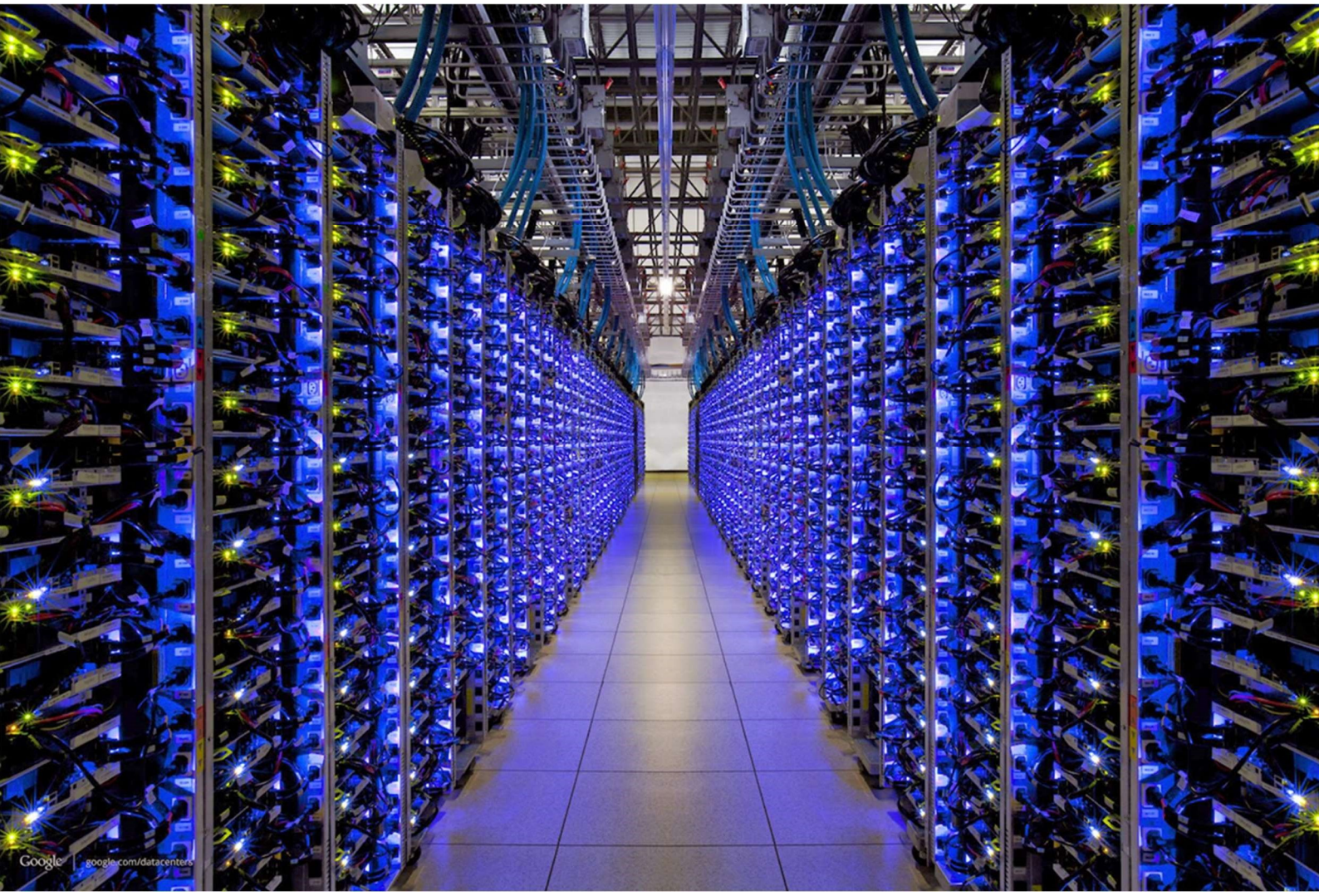
Eindrapport

Quickscan van de gevolgen van de voorgestelde verordeningen Interoperabiliteit voor de Nederlandse uitvoeringspraktijk



Andersson Elffers Felix

Maliebaan 16
Postbus 85198
3508 AD Utrecht

+31 30 236 30 30
mail@aef.nl
www.aef.nl

Kamer van Koophandel
30096560

Datum
1 oktober 2018

Opdrachtgever
Ministerie van Justitie en Veiligheid, Directie Europese en Internationale Aangelegenheden

Contact
Tiddo Folmer
Michiel Ehrismann
Amber van Suijlekom

Referentie
GJ189/rapportage quickscan interoperabiliteit

Inhoud

1 Inleiding

Eind 2017 heeft de Europese Commissie twee verordeningen uitgevaardigd die samen een wetgevingsvoorstel omvatten over interoperabiliteit tussen centrale EU-informatiesystemen. Het gaat om systemen op het gebied van grensbeheer, veiligheid en migratie. De verordeningen bieden een juridisch kader voor vier nieuwe componenten die centrale EU-informatiesystemen nauwer met elkaar laten communiceren en samenwerken.

De betreffende informatiesystemen worden op Europees niveau beheerd, maar Nederlandse (uitvoerings)organisaties in de veiligheid- en migratieketen werken ook met deze systemen. Daarom wordt ook de Nederlandse uitvoeringspraktijk geraakt; mogelijk verandert de manier waarop Nederlandse organisaties werken of verandert de manier waarop hun ICT-ondersteuning en andere bedrijfsvoering werkt.

Andersson Elffers Felix (AEF) is gevraagd om met een quickscan in grote lijnen de impact van de verordeningen op de Nederlandse uitvoeringspraktijk in kaart te brengen. In deze rapportage staan de bevindingen en aanbevelingen uit de quickscan beschreven.

1.1 De verordeningen

De verordeningen vormen samen de juridische basis voor vier ICT-componenten waarmee de interoperabiliteit van centrale EU-informatiesystemen wordt gerealiseerd. De eerste verordening geldt voor het Schengengebied; de tweede voor het Europese Unie gebied:

- ***COM (2017) 793:*** *voorstel voor een verordening van het Europees Parlement en de Raad inzake de vaststelling van een kader voor interoperabiliteit tussen EU-informatiesystemen (grenzen en visa) en tot wijziging van Beschikking 2004/512/EG van de Raad, Verordening (EG) nr. 767/2008, Besluit 2008/633/JBZ van de Raad, Verordening (EU) 2016/399 en Verordening (EU) 2017/2226*
- ***COM (2017) 794:*** *voorstel voor een verordening van het Europees Parlement en de Raad betreffende de vaststelling van een kader voor interoperabiliteit tussen EU-informatiesystemen (politiële en justitiële samenwerking, asiel en migratie)*

De verordeningen schetsen een kader om de informatie-uitwisseling tussen autoriteiten te uniformeren en standaardiseren. Het doel hiervan is onder meer de identificatieprocessen te vereenvoudigen en de kwaliteit van gegevens te verbeteren. Dit moet de informatiepositie van autoriteiten versterken en daarmee het beheer van buitengrenzen van het Schengengebied verbeteren en bijdragen aan de interne veiligheid van de EU.

Tegelijkertijd met deze twee verordeningen gericht op interoperabiliteit, liggen er ook voorstellen om nieuwe EU-informatiesystemen te introduceren of te updaten.

1.2 Vraagstelling

Opdracht

De quickscan is gespecificeerd als een onderzoek dat de gevolgen van de voorstellen voor de eindgebruikers en hun organisaties zowel op het terrein van taakuitvoering als op het terrein van (randvoorwaardelijke) bedrijfsvoering in beeld brengt. De centrale opdracht luidde:

> *Een impactanalyse in de vorm van een quickscan m.b.t. de twee EU-voorstellen die nieuwe elementen bevatten om interoperabiliteit tussen centrale EU-informatiesystemen op het terrein van migratie, grensbeheer en veiligheid te realiseren.*

AEF maakt hierbij onderscheid tussen *structurele effecten* en *éénmalige effecten* op primaire processen en bedrijfsvoering enerzijds en *éénmalige effecten* in de implementatie- en transitieperiode anderzijds. De nadruk in deze quickscan ligt op de structurele effecten; waar nodig worden de belangrijkste eenmalige invoeringseffecten opgemerkt.

De rapportage van de quickscan kan een voorzet vormen voor een goede gezamenlijke procesgang tussen de betrokken organisaties. Onderlinge afstemming en samenwerking is in het implementatietraject van belang gezien de veranderingen en aanpassingen waar de verordeningen voor zorgen. Daarbij moeten cruciale keuzes voor de inrichting van het brede ICT-veld gemaakt worden. Deze quickscan kan ondersteuning bieden bij dat proces.

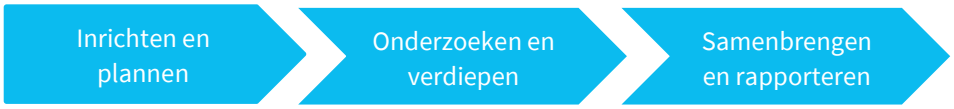
Scope

Binnen scope van deze quickscan zijn de structurele en eenmalige effecten van de verordeningen Interoperabiliteit op de Nederlandse uitvoeringspraktijk. Daarbij is er aandacht voor de effecten op de primaire processen (bijvoorbeeld handhaving door een agent op straat of visumverstrekking door een ambassademedewerker) en op bedrijfsvoering (bijvoorbeeld de invulling van ICT, personeel, organisatie, voorlichting en training).

Geen onderdeel van deze quickscan zijn de juridische toetsing van de verordeningen aan wet- en regelgeving en de consequenties voor Europese uitvoeringsorganisaties. Ook de voorstellen om nieuwe EU-informatiesystemen op te zetten en andere te updaten, zijn buiten de scope van deze quickscan.

1.3 Aanpak

De quickscan is door AEF opgezet en uitgevoerd tussen eind juni en midden september 2018. Dat is gebeurd in drie achtereenvolgende stappen:



Stap 1. Inrichten en plannen

In de eerste stap is de quickscan opgezet, waarbij in beeld is gebracht welke Nederlandse (uitvoerings)organisaties in potentie het meest geraakt worden door de verordeningen.

Er zijn acht organisaties/organisatieonderdelen betrokken bij deze quickscan:

- Nationale Politie (NP)
- Koninklijke Marechaussee (KMar)
- Immigratie- en Naturalisatiedienst (IND)
- Dienst Terugkeer & Vertrek (DT&V)
- Ministerie van Buitenlandse Zaken (BZ)
- Openbaar Ministerie (OM)
- Justitiële Informatiedienst (Justid)
- Directie Regie Migratieketen (DRM)

Stap 2. Onderzoeken en verdiepen

In de tweede stap heeft AEF de situatie in kaart gebracht van alle geraakte processen, SPIOFACH[1]-breed, bij de betrokken organisaties. Van daaruit heeft AEF onderzocht hoe deze processen veranderen door de verordeningen.

AEF heeft in de quickscan gebruik gemaakt van drie type bronnen:

- **Interviews** met betrokken partners voor een kwalitatieve duiding van de impact op interne processen en op de effectiviteit van geleverde diensten en samenwerkingen. Voor dit onderzoek zijn ook interviews gehouden met programma Grenzen en veiligheid en de Autoriteit Persoonsgegevens.
- **Documentanalyse**, ter duiding en prioritering van de effecten van de verordeningen op de processen, systemen en diensten van de betrokken partners.
- **Bijeenkomsten begeleidingsgroep** met een selectie van betrokken partners, om het onderzoek effectief richting te geven en om onze bevindingen en conclusies te toetsen.

Stap 3. Samenbrengen en rapporteren

In de laatste stap van de quickscan heeft AEF de laatste analyses uitgewerkt en een conceptrapportage geschreven. De rapportage bevat een overzicht van de structurele en eenmalige effecten op de taakuitvoering en bedrijfsvoering van de organisaties. Tevens biedt de rapportage een overzicht van de belangrijkste keuzes die in het implementatietraject gemaakt moeten worden en beschrijft het de aanbevelingen voor afstemming en samenwerking.

Begeleidingsgroep

De quickscan is gevolgd door een begeleidingsgroep met vertegenwoordigers van de betrokken uitvoeringsorganisaties en beleidsmakers. Deze begeleidingsgroep is driemaal bijeen gekomen.

1.4 Leeswijzer

In deze rapportage zijn de uitkomsten van de impactanalyse beschreven.

- In **hoofdstuk 2** leest u over het vertrekpunt voor de analyse: de inhoud en het tijdspad rond de verordeningen en de stand van zaken bij Nederlandse uitvoeringsorganisaties.
- **Hoofdstuk 3** beschrijft de (verwachte) structurele effecten van de verordeningen op de uitvoeringspraktijk in Nederland.
- In **Hoofdstuk 4** leest u welke eenmalige effecten optreden wanneer de verordeningen geïmplementeerd worden.
- In **hoofdstuk 5** beschrijven we welke vervolgstappen wij zien voor betrokken organisaties en welke besluiten er op dit moment genomen moeten worden.
- In **hoofdstuk 6** worden de analyses uit de voorgaande hoofdstukken gecombineerd in de conclusie, die leidt tot het advies van AEF.

Het verschil tussen de structurele effecten in hoofdstuk 3 en de eenmalige effecten in hoofdstuk 4 is dat eerstgenoemde effecten gaan over het effect als de verordeningen volledig van kracht zijn. De laatstgenoemde effecten beschrijven de acties om dat te bereiken.

[1] SPIOFACH is gedefinieerd als Security, Personeel, Informatievoorziening, Organisatie, Financiën, Automatisering, Communicatie, Huisvesting.

2 Vertrekpunt

Dit hoofdstuk schetst de verordeningen en het huidig voorgenomen proces om die in te voeren.

2.1 Componenten

De verordeningen hebben betrekking op zes[2] centrale Europese informatiesystemen in de veiligheids- en migratieketen:

- **SIS:** het Schengeninformatiesysteem II (hier kortweg SIS) bevat signaleringen van personen en voorwerpen die relevant zijn voor autoriteiten in het Schengengebied.
- **VIS:** het Visuminformatiesysteem bevat gegevens over houders van een visum voor kort verblijf in het Schengengebied.
- **Eurodac:** dit is het Europese register van vingerafdrukgegevens van asielzoekers en van derdelanders die de buitengrenzen onrechtmatig hebben overschreden.
- **EES:** het Inreis- en Uitreissysteem gaat sommige binnenkomende en uitgaande reizen van derdelanders bij het overschrijden van de Schengenbuitengrenzen registeren.
- **ETIAS:** Met het Europees systeem voor reisinformatie en -autorisatie kunnen niet-visumplichtige vreemdelingen een autorisatie krijgen voor het Schengengebied.
- **ECRIS-TCN:** Het Europees strafregister voor derdelanders wordt het centraal systeem voor justitiële informatie over derdelanders die onherroepelijk zijn veroordeeld in de EU.

SIS, VIS en Eurodac krijgen de komende jaren grote updates. EES, ETIAS en ECRIS-TCN worden zelfs voor het eerst opgezet. De Europese Commissie heeft vier componenten voorgesteld om de onderlinge interoperabiliteit van deze systemen te verbeteren:

1. **European Search Portal (ESP):** een zoekfunctie waarmee de informatiesystemen gelijktijdig worden bevraagd.
2. **shared Biometric Matching Service (sBMS):** een centrale component voor het opvragen en vergelijken van biometrische gegevens.
3. **Common Identity Repository (CIR):** een centraal gegevensbestand met persoonsgegevens van derdelanders geregistreerd in de bovenstaande systemen (behalve SIS).
4. **Multiple-identity detector (MID):** een functie die koppelingen creëert tussen overeenkomende identiteitsgegevens in de EU-informatiesystemen.

Naast de vier componenten worden ook ondersteunende functies voorgesteld, bijvoorbeeld voor het genereren van statistische informatie.

[2] Naast deze zes systemen gelden kleine delen van de verordeningen ook voor de systemen van Europol en Interpol. Die delen bespreken we alleen waar relevant. Vanwege de leesbaarheid spreken we anders van ‘de zes’ systemen.

2.2 Beoogd tijdspad voor wetgeving- en implementatietraject

Er ligt nog geen definitief tijdspad voor invoering van de verordeningen. Hieronder beschrijven we de huidige voorstellen voor een tijdspad. Die zijn nog niet bekrachtigd en kunnen nog veranderen. Het tijdspad voor Interoperabiliteit is nauw verbonden met de trajecten waarbij de EU-informatiesystemen worden geüpdatet of opgezet.

2016 – 2017

Voorstellen voor interoperabiliteit zijn niet nieuw: in 2004 riep de Europese Raad al op om SIS, VIS en Eurodac beter te verbinden. De verordeningen vinden hun oorsprong in de *EU routekaart informatievoorziening en informatie-uitwisseling* van 2016. Deze routekaart bevatte voorstellen om SIS, Eurodac en VIS bij te werken en om EES, ETIAS en ECRIS-TCN op te zetten.

Om de samenhang tussen deze systemen te waarborgen, werd ook voorgesteld om componenten voor interoperabiliteit te introduceren. De Europese Commissie heeft op 12 december 2017 de voorgestelde verordeningen Interoperabiliteit gepubliceerd.

2018 – 2019

De Tweede Kamer heeft kort een behandel-voorbehoud aangehouden. Dit is in maart 2018 beëindigd. Daarbij is onder meer afgesproken dat de quickscan met de Tweede Kamer wordt gedeeld. Besluitvorming komt uiteindelijk bij de Europese organen. De huidige verwachting is dat het Europees Parlement in de loop van 2019 de laatste goedkeuring kan geven, waarna formeel het implementatietraject start.

Op dat moment zijn de verordeningen rond individuele systemen al besproken, met uitzondering van VIS dat enkele maanden later volgt. In de praktijk wordt van lidstaten echter verwacht dat ze al technisch uitgewerkte implementatieplannen hebben klaarliggen.

2020 – 2021

Ervan uitgaand dat zowel de updates als interoperabiliteit worden goedgekeurd, zou de technische ontwikkeling veelal plaatsvinden in 2020 en 2021. Als gezegd dienen de plannen hiervoor echter al eerder (en dus in de komende tijd) te worden uitgewerkt.

Tijdens deze periode zouden de eerste componenten rond interoperabiliteit worden ontwikkeld, vaak parallel met de ontwikkeling van nieuwe systemen. Zo kan de CIR bijvoorbeeld eerst worden ontwikkeld voor EES en later uitgebreid naar de andere systemen. Ontwikkeling van de MID zou vanaf 2021 starten, als laatste van de vier componenten.

2022 – 2023

Volgens de huidige planning zouden (de updates van) de EU-informatiesystemen begin 2022 live gaan; het EES mogelijk eerder. Enige tijd daarna gaan ook de interoperabiliteit componenten ‘live’; sBMS en CIR het eerst; vervolgens ESP (in volledige vorm) en MID als laatste.

De bovenstaande planning is voorlopig van aard. Als deze voorlopige planning gerealiseerd wordt, hebben Nederlandse organisaties ongeveer een jaar voorbereidingstijd en daarna circa drie jaar om de componenten in samenwerking met Europese organisaties te implementeren.

2.3 Huidige stand van zaken in Nederland

De inrichting van de interoperabiliteit componenten verloopt grotendeels parallel aan de updates of ontwikkeling van de informatiesystemen. Dit zijn stuk voor stuk complexe ICT-projecten voor Nederlandse uitvoeringsorganisaties. Om deze inspanningen te coördineren, heeft het ministerie van JenV een coördinatieprogramma opgezet: het programma Grenzen en veiligheid.

AEF heeft in de ronde langs de uitvoeringsorganisaties geconstateerd dat er voor de uitvoering nog behoorlijke stappen gezet moeten worden. Alle uitvoeringsorganisaties hebben de verordeningen Interoperabiliteit ‘op de radar’ en zien dat de verordeningen consequenties gaan hebben voor hun primaire processen en bedrijfsvoering. Voor de implementatie is in veel gevallen al projectleiding ingericht of is men druk bezig die projectleiding te realiseren.

Er moeten dus nog wel verdere concrete stappen gezet worden om de precieze consequenties per organisatie in beeld te krijgen. Voor interoperabiliteit zijn er op dit moment nog geen impactanalyses vanuit de betrokken individuele organisaties beschikbaar. Dit betekent dat deze quickscan geen gebruik kon maken van bestaand onderzoek op organisatieniveau. De effecten die we in de volgende hoofdstukken bespreken, zijn dus, naast de studie van algemenere documenten, gebaseerd op expertinschattingen uit interviews en bijeenkomsten.

3 Structurele effecten

In dit hoofdstuk leest u hoe de nieuwe componenten het werk van Nederlandse uitvoeringsorganisaties veranderen. Dat gaat om **primaire processen** maar ook om de ondersteuning op het gebied van **bedrijfsvoering** (waaronder ICT).

3.1 Veranderingen per component

Zoals beschreven in hoofdstuk 2, introduceren de verordeningen vier nieuwe componenten.

3.1.1 European Search Portal

Het European Search Portal is een technische component waarmee gebruikers de zoekopdrachten tegelijk kunnen plaatsen in de verschillende EU-informatiesystemen. Het ESP geleidt zoekopdrachten vanuit een nationaal systeem[3] door naar de informatiesystemen en geeft de zoekresultaten terug aan de eindgebruiker.

Het ESP kan alle zes genoemde EU-informatiesystemen doorzoeken. Het is tevens de enige component die ook gaat gelden voor de systemen van Europol en Interpol. De impact op de Nederlandse uitvoeringspraktijk is gelijk aan die van de impact vanuit de zes EU-systemen.

Veel van de EU-informatiesystemen zijn in de eerste plaats bedoeld voor beheer van de buitengrenzen. Rechtshandhaving is een secundaire doelstelling van de onderliggende migratiesystemen (zoals EES, ETIAS, VIS en Eurodac). Daarom werkt de toegang tot de ESP-zoekresultaten voor rechtshandhavers via een tweetrapsbenadering: medewerkers voeren een zoekopdracht in en krijgen dan te zien of er informatie over de persoon waar ze naar zoeken in een register staat (hit / no-hit). Bij een hit kunnen de rechtshandhavers, als ze voldoende toegangsrechten hebben, nagaan welke informatie er geregistreerd is.

Zolang Nederlandse uitvoeringsorganisaties hun gebruikelijke registers doorzoeken, veranderen de **primaire processen** niet sterk. Veel organisaties hebben al een zoekfunctie die tegelijk verschillende registers kan doorzoeken. In andere landen kan het gebeuren dat overheidsmedewerkers zes keer een zoekopdracht invoeren. Dan is het ESP een grote stap vooruit. Maar die stap is in Nederland feitelijk al gezet.

Er zijn wel veranderingen in het geval uitvoeringsorganisaties aanvullende toegangsrechten nodig hebben, bijvoorbeeld voor registers waar ze normaal gesproken geen toegang toe hebben. Een voorbeeld is het voorkomen van terrorisme door de Politie of Marechaussee. In

[3] Systemen op nationaal niveau worden vanwege de leesbaarheid in dit rapport aangeduid als ‘nationaal systeem’. Er zijn minstens acht organisaties op dit niveau. Die kennen dus allemaal hun eigen ‘nationaal systeem’.

de huidige situatie moeten ze dan voor elk register apart toegang aanvragen bij een zogeheten Central Access Point. In de nieuwe situatie ontstaat er een juridisch kader om een Central Access Point toegang te vragen om in één keer met het ESP alle registers tegelijk te doorzoeken. Toegang tot de informatie in de onderliggende registers gaat dan (nog steeds) volgens de toegangsvoorwaarden zoals vastgesteld in de onderliggende wetgevende instrumenten van die informatiesystemen.

Op het gebied van **bedrijfsvoering** brengt het ESP verdere veranderingen met zich mee. Het ESP gaat koppelen met de nationale systemen via een Nationaal Uniforme Interface, die eu-LISA gaat leveren en beheren. Het is nog niet helemaal duidelijk hoe deze er uit gaat zien. Daarnaast zullen de organisaties waarschijnlijk, als 'back-up', ook de oude (directe) lijnen in stand moeten houden. De organisaties moeten dus meer ICT-koppelingen onderhouden.

Het ICT-beheer van de ESP-component zelf ligt bij EU-agentschap eu-LISA en brengt geen beheerkosten voor Nederland met zich mee. Dit geldt ook voor de andere drie componenten.

3.1.2 shared Biometrics Matching Serivce

Elk EU-informatiesysteem dat biometrische gegevens bevat, heeft momenteel een eigen matching service om die gegevens te doorzoeken. Het shared Biometrics Matching Service vervangt deze aparte zoekfuncties met één overkoepelende zoekfunctie.

De **primaire processen** van Nederlandse uitvoeringsorganisaties kunnen dus alleen veranderen als ze meerdere biometrische registers tegelijk mogen doorzoeken. Dat gebeurt het vaakst in de opsporingsprocessen van de Nationale Politie. Echter, de Politie kan nu al meerdere biometrische registers tegelijk doorzoeken[4], via het zogeheten zuilonderzoek (waartoe overigens niet iedereen gemachtigd is).

Op zichzelf heeft de matching service daarmee geen groot effect. Echter, sBMS is wel een noodzakelijke randvoorwaarde om de andere componenten goed te laten werken. Die componenten maken het mogelijk om misbruik van meerdere identiteiten op te sporen, waarbij biometrische gegevens leidend zijn. In dat opzicht is sBMS een verrijking.

Op de **bedrijfsvoering** heeft sBMS geen groot effect. In principe kunnen Nederlandse organisaties hun eigen matching services afschaffen en sBMS gebruiken. In tegenstelling tot bij het ESP zijn nationale autoriteiten hier niet verplicht om hun eigen systemen als back-up in de lucht te houden. Daarmee verschuift er enig beheerwerk van Nederland naar Europa. Ook vraagt sBMS op zichzelf niet om extra voorlichting bovenop wat er al voor het ESP gebeurt.

3.1.3 Common Identity Repository

De Common Identity Repository is oorspronkelijk ontworpen als centraal gegevensbestand met de persoonsgegevens van derdelanders. De precieze (technische) invulling van CIR kent echter nog veel vraagtekens. Zo vond een analyse van het Europees Parlement[5] in april 2018 het onduidelijk of CIR gezien dient te worden als een eigen database. In elk geval zou CIR wel

[4] Dat geldt uiteraard alleen voor de registers die nu al bestaan. In de komende jaren worden er nieuwe biometrische registers opgezet, en dankzij sBMS zijn er geen inspanningen nodig op nationaal niveau om ook die te kunnen doorzoeken.

[5] Interoperability of Justice and Home Affairs Information Systems, Policy Department for Citizens' Rights and Constitutional Affairs, 2018

'schotten' kennen om de oorspronkelijke toegangsrechten in stand te houden en bovendien mogen er geen nieuwe gegevens verzameld worden die in de huidige situatie nog niet verzameld worden.

De effecten van CIR zijn dus nog niet vast te stellen zonder verdere details vanuit Europa. In principe zou (een systeem dat functioneert als) één identiteitsregister de **primaire processen** moeten vergemakkelijken. Er is dan namelijk minder kans op overlappende, conflicterende registraties van identiteit. Echter, CIR wordt niet het *enige* register: er blijven andere identiteitsregisters bestaan in nationale registers (en in het SIS, al wordt daar de MID voor ingesteld). De verwachting van de betrokken organisaties is dat het werk van hun medewerkers ook niet wordt versneld.

De **bedrijfsvoeringsprocessen** worden aan de ICT-kant iets gemakkelijker omdat er minder verschillende koppelingen nodig zijn om identiteitsinformatie uit te wisselen. Het effect daarvan is klein. In voorlichting en communicatie kan waarschijnlijk dezelfde boodschap worden uitgedragen als voor het ESP.

De belangrijkste effecten van het CIR zitten in de risico's: wanneer dit ene register onverhoopt niet beschikbaar zou zijn, zit een groot deel van de Nederlandse veiligheid- en migratieketen zonder informatie vanuit Europa. Zonder die informatie kan de keten bijvoorbeeld minder effectief terrorisme voorkomen. Paragraaf 3.2 gaat verder op dit risico in.

3.1.4 Multiple Identity Detector

De Multiple Identity Detector detecteert of er meerdere identiteiten gekoppeld zijn aan eenzelfde set paspoort- of biometrische gegevens. Als dat het geval is, creëert de MID een link tussen die gegevens. De nationale autoriteit moet aan die (geel gekleurde) link vervolgens een kleurcode toewijzen die aangeeft wat er aan de hand is:

- Een witte link geeft aan dat er sprake is van één bonafide (goedbedoelend) persoon.
- Een groene link geeft aan dat er sprake is van twee bonafide personen.
- Een rode link geeft aan dat er sprake is van onrechtmatig gebruikte identiteiten.

Met de MID ontstaat een nieuw **primair proces** waarbij uitvoeringsorganisaties moeten nagaan waarom er sprake is van overeenkomende identiteiten in de Europese registers. Vervolgens moeten ze aangeven hoe er nu en later met deze persoon wordt omgegaan.

Dit nieuwe proces kost extra tijd. Ook nu al voeren de uitvoeringsorganisaties wel eens onderzoek uit naar meerdere identiteiten, maar nog niet op basis van een vaste aanleiding (een alarmsignaal in een ICT-systeem). Bovendien is de verwachting dat dit nu veel vaker gaat gebeuren. Het is nog niet duidelijk hoe dit proces rond gele links er precies uit gaat zien, maar wel dat het impact op de uitvoeringsorganisaties heeft.

Het verwerken van gele links kost tijd, maar is van grote waarde. De uitvoeringsorganisaties geven aan dat de georganiseerde misdaad, mensensmokkelaars en mogelijk ook terroristen van meerdere identiteiten gebruikmaken. Een impactanalyse van de Europese Commissie schatte hun aantal op 500.000 per jaar[6]. Het tegengaan van meerdere identiteiten kan de grens-, visum- en opsporingsprocessen versterken. De kans dat malafide personen daarmee worden gedetecteerd, neemt toe.

[6] Impact assessment; Accompanying the document [...] on establishing a framework for interoperability between EU information systems (…) part 2, European Commission, 2017, p. 17.

De effecten van het nieuwe primaire proces op de **bedrijfsvoering** zijn groot. De verwachting is dat de verwerking van gele links deels bij medewerkers in het primair proces wordt gelegd. Zij krijgen dan een 'frontoffice'-taak om eenvoudige gevallen op te lossen. Uitvoerings-organisaties zullen op zijn minst hun medewerkers goed hiervoor moeten trainen.

Om de minder eenvoudige gevallen op te lossen, zou Nederland waarschijnlijk één of meerdere gespecialiseerde afdelingen opzetten om gele links te verwerken. Deze afdeling(en) functioneert of functioneren dan als 'backoffice'. Er is nu nog geen besluit over welke afdelingen dat zijn. In elk geval vragen nieuwe of uitgebouwde afdelingen om reallocatie van personeel, ICT, financiën, administratieve structuren, huisvesting en securitymaatregelen.

3.2 Operationele risico's

De vorige paragraaf beschreef de effecten wanneer de nieuwe componenten volgens plan functioneren. Er ontstaan echter ook risico's voor de situatie wanneer ze (tijdelijk) niet volgens plan functioneren. Uit het onderzoek komen de volgende risico's naar voren:

- **Datakwaliteit:** door de nieuwe componenten wordt Nederland afhankelijker van de kwaliteit van registratie in andere landen. Wanneer die kwaliteit niet goed is, ontstaan er veel valse positieve of negatieve links en zoekresultaten. De verordeningen besteden hier aandacht aan en stellen maatregelen voor, maar de Nederlandse uitvoeringsorganisaties zien dit toch als risico, vooral bij de Multiple Identity Detector.
- **Rolvermenging:** de Europese verordeningen onderscheiden verschillende rollen, zoals 'judicial authorities', 'law enforcement authorities' en 'customs authorities'. Die Europese indeling past echter niet precies op de Nederlandse praktijk: soms wordt één rol door verschillende Nederlandse organisaties vervuld, of vervult één organisatie meerdere rollen. Als verschillende rollen door elkaar gaan lopen, wordt het moeilijker om op een consequente manier toegangsrechten te verlenen. De handhaving hiervan wordt belangrijker.
- **Performance:** de snelheid waarmee systemen reageren is hun 'performance'. De Europese Commissie stelt ambitieuze doelen voor de performance van de nieuwe componenten, maar het is nog onzeker of die gehaald worden. Als de componenten trager reageren, gaan daarmee de processen in de Nederlandse praktijk langzamer. Dit is met name risicovol in het grensproces, waar dit al snel langere wachttijden geeft.[7]
- **Beschikbaarheid:** het deel van de tijd dat informatiesystemen beschikbaar zijn, staat bekend als hun 'uptime'. Ook hiervoor geldt dat het onzeker is of de Europese componenten nagenoeg altijd beschikbaar gaan zijn. Als EU-informatiesystemen tijdelijk stilliggen vanwege storingen, kan dat de primaire processen sterk verstoren. Nederland heeft zich overigens binnen Europa sterk ingezet voor voldoende terugvalopties.
- **Identiteitsverwisseling:** soms staan goedwillende burgers verkeerd geregistreerd in de systemen. Dit overkomt vooral de slachtoffers van ID-fraude: iemand misbruikt hun identiteit. De betrokken organisaties waarschuwen dat het met interoperabiliteit moeilijk kan worden om verkeerde registraties te herstellen en dat de impact groot kan zijn (goedwillende burgers worden ten onrechte vaker onderworpen aan nader (intensiever) onderzoek). Daar staat tegenover dat foute registratie in sommige omstandigheden sneller kan worden rechtgezet.

[7] Een opmerkelijk gegeven is dat als het ESP traag werkt, de Nederlandse processen trager worden. In de huidige situatie hebben de Nederlandse organisaties zelf zoekfuncties met dezelfde capaciteit en hogere performance. De verordeningen stellen echter dat zoekopdrachten in principe via het ESP gaan lopen, met de nationale functie alleen als achtervang.

Beheersmaatregelen bij deze risico's komen van verschillende niveaus, waaronder Europa, nationaal en individuele organisaties. In Nederland dient programma Grenzen en veiligheid de nationale coördinatie te verzorgen en het contact met Europa te onderhouden. Tegelijk dienen de Nederlandse uitvoeringsorganisaties voor zichzelf beheersmaatregelen uit te werken. In zijn algemeenheid verdient het aanbeveling om daarbij niet alleen naar technische beheersmaatregelen (zoals back-upsystemen) te kijken maar ook naar organisatorische maatregelen (zoals noodprocedures) omdat Nederland op technisch gebied afhankelijker wordt van Europa.

3.3 Structurele opbrengsten en kosten

Uit het onderzoek blijkt dat het op dit moment te vroeg is om opbrengsten en kosten te berekenen. Alle beleidsmakers en uitvoeringsorganisaties geven aan dat er daarvoor nog te veel onzekerheden zijn (zie hoofdstuk 5).[8] Er is een eerste inschatting in de Europese impactanalyses, maar die wordt door hen niet herkend en is bovendien niet onderbouwd.

Wel kan dit onderzoek alvast de bovengenoemde effecten ordenen op indicatieve grootte. Een dergelijk getal geeft al een gevoel voor de belangrijkste financiële elementen. De onderstaande tabel bevat de bij de uitvoeringsorganisaties getoetste ordening. Daarbij is het nuttig op te merken dat de kosten en opbrengsten bij verschillende ketenpartijen vallen. Soms betreft het zelfs maatschappelijke opbrengsten zonder direct financieel effect op de uitvoeringsorganisaties.

Effect	Toelichting	Orde grootte op jaarbasis
Structurele kosten		
Verwerken gele links	**Het verwerken van MID links vraagt meer structurele capaciteit (eerste schattingen denken aan minstens tientallen fte)**	**Miljoenen**
Ketenpartner systemen	De nationale systemen bieden toegang tot de Europese componenten en hun onderhoud wordt iets complexer.	Honderd-duizenden
Koppelvlakken	Het onderhoud van koppelingen tussen nationaal en Europees niveau wordt duurder omdat er nieuwe koppelingen ontstaan.	Tienduizenden
Instructies	Instructies over de werkwijze worden iets complexer omdat die o.a. de tweetrapstoegang extra moeten uitleggen[9].	Tienduizenden
Structurele opbrengsten		
Meerdere identiteiten	**Het tegengaan van misbruik van meerdere identiteiten wordt effectiever. Dit scheelt aanzienlijk in maatschappelijke kosten.**	**Miljoenen**
CIR en sBMS-koppelingen	Zonder interoperabiliteit zou elk systeem eigen identiteits- en biometrische gegevens hebben; met interoperabiliteit niet.	Tienduizenden

[8] Bovendien zijn de kosten voor interoperabiliteit moeilijk los te zien van de kosten voor updates van individuele registers.

[9] Dit betreft alleen de structurele situatie. De eenmalige omscholing van zittende medewerkers op het moment dat de maatregelen worden ingevoerd, staat apart beschreven in hoofdstuk 4. De kosten worden laag ingeschat omdat dit soort instructies kunnen meegenomen in bestaande processen voor instructies.

Deze inschattingen gaan uit van de totale kosten voor de Nederlandse veiligheids- en migratieketen. Het effect van het optreden van risico's (paragraaf 3.2) of het nemen van beheersmaatregelen is hierin nog niet gekwantificeerd. Er wordt momenteel nog geen dekking vanuit Europese fondsen geraamd.

4 Eenmalige effecten bij implementatie

In dit hoofdstuk leest u welke inspanningen er (eenmalig) verricht moeten worden om de verordeningen te implementeren. Ook beschrijven we welke risico's daarbij gelden.

4.1 Implementatiestappen

Implementatie van de Europese verordeningen vindt plaats over een periode van twee à drie jaar, zie paragraaf 2.2. In die tijd moet een aantal activiteiten worden uitgevoerd.

Bijwerken ketenpartnersystemen

Alle betrokken uitvoeringsorganisaties kennen een web van onderling verbonden informatie-systemen, databases en registers op nationaal niveau. Niet al die systemen hebben een eigen interface. Vaak gebruiken de medewerkers in het primair proces maar één of twee centrale systemen waarmee ze bijna alle informatie ontsluiten. Voorbeelden zijn de BVV, BVI-IB of IOB.[10]

Deze ketenvoorzieningen en ketenpartnersystemen moeten worden bijgewerkt om aan de verordeningen te voldoen. De precieze veranderingen daarover zijn nog niet bekend en verschillen waarschijnlijk per systeem. Ook zijn er naar verwachting een nieuw berichtenboek (op basis van de UMF standaard) en nieuwe schermen in de interface nodig om de extra informatie te kunnen weergeven. Tenslotte moet de logging (registratie van activiteiten van gebruikers) worden aangepast.

De ketenpartnersystemen moeten waarschijnlijk allemaal een nieuwe functie kennen om de gele links vanuit de Multiple Identity Detector te verwerken. Hoewel de precieze inspanning nog niet bekend is, zal het bijwerken van de centrale Nederlandse systemen een relatief grote wijziging zijn voor de betrokken IV-/ICT-afdelingen. Het is aannemelijk (maar nog niet zeker) dat de achterliggende informatiesystemen niet of nauwelijks hoeven worden bijgewerkt.

Bijwerken koppelingen

De betrokken Nederlandse systemen zijn via koppelvlakken en ketenvoorzieningen verbonden met de Europese registers. Deze koppelvlakken moeten worden bijgewerkt. De precieze activiteiten zijn nog niet te overzien. Nog sterker dan bij de centrale informatiesystemen zijn de Nederlandse organisaties hier afhankelijk van meer informatie vanuit het betrokken EU-agentschap eu-LISA. Nadat de verordening is vastgesteld wordt begonnen met het verder uitwerken van het berichtenboek (het zogeheten *Interface control document*).

[10] BVV: Basisvoorziening vreemdelingen, van DRM. BVI-IB: Basisvoorziening Informatie-Integrale Bevraging, van de Nationale Politie. IOB: Informatie Ondersteund Beslissen, van Buitenlandse Zaken.

Opleiding en instructie

Door de komst van de interoperabiliteit componenten veranderen de processen. De grootste verandering is de tweetrapstoegang voor rechtshandhavers tot de migratiesystemen. Die verandert de werkwijze van medewerkers in het primair proces. Ze gaan hun informatiesystemen op een andere manier gebruiken. Dit vraagt om nieuwe instructies en opleiding aan alle medewerkers om de nieuwe werkwijze te volgen.

Naast het eenmalige bijscholen van alle medewerkers, is er ook verandermanagement nodig om de structurele instructies bij te werken, bijvoorbeeld voor medewerkers die nieuw instromen. Dit vraagt een aanpassing in het reguliere scholingsbeleid.

Bijwerken nieuwe processen

Ook worden delen van het autorisatiebeleid bijgewerkt. De hoofdlijn verandert niet eens zo sterk want de verordeningen willen de toegang tot data weliswaar stroomlijnen, maar niet herzien. Ze willen in principe geen nieuwe data creëren. Dat verkleint de impact op gegevensbescherming. Hierop zijn echter uitzonderingen: de gele links van de MID bijvoorbeeld zijn mogelijk wél persoonsgegevens.

Tenslotte moeten documenten zoals het *Protocol Identificatie en Labeling* en andere afspraken over processen worden bijgewerkt.

Opzetten verwerkingsproces

Zoals beschreven in sectie 3.1.4 ontstaat er een nieuw proces voor verwerken van gele links vanuit de Multiple Identity Detector. AEF verwacht dat ervoor gekozen wordt om dit bij één of enkele gespecialiseerde afdeling(en) te beleggen. Deze afdelingen moeten worden opgezet of sterk worden uitgebreid. Dat vraagt werving van nieuwe medewerkers en speciale projecten.

4.2 Implementatierisico's

Het implementatietraject kent aan Nederlandse zijde een aantal risico's. Uit het onderzoek komen drie risico's het sterkst naar voren:

- **Stapeling van complexe ICT-projecten:** in de komende jaren moeten de Nederlandse uitvoeringsorganisaties niet alleen de verordeningen Interoperabiliteit verwerken, maar ook updates van SIS, VIS, Eurodac doorvoeren en EES, ETIAS en ECRIS-TCN opzetten.[11] Dat zijn op zichzelf al complexe ICT-projecten, maar de onderlinge afhankelijkheden met Interoperabiliteit maken die nog complexer. In dit veld, met een groot aantal spelers, zal het moeilijk worden een logisch implementatiepad op te zetten.
- **Hoeveelheid links:** op voorhand kunnen de uitvoeringsorganisaties nog niet inschatten hoeveel links de Multiple Identity Detector gaat afgeven. Los van de vraag of die gele links terecht zijn (zie paragraaf 3.2) kan een groot aantal links op zichzelf een probleem zijn bij de implementatie. Het wordt dan namelijk moeilijker om op tijd afdelingen in te richten die deze hoeveelheid kunnen verwerken.
- **Afhankelijkheid van eu-LISA:** het Europese agentschap dat verantwoordelijk is voor de implementatie, eu-LISA, staat voor een grote opgave. Ook eu-LISA moet bovenstaande projecten doorvoeren, maar op Europees niveau zijn die projecten nog groter. Het is een

[11] En tegelijk lopen er ook nog vergelijkbare trajecten die niet via eu-LISA lopen, zoals invoering van de richtlijn Passenger Name Records.

jong en vrij klein agentschap en het is nog onzeker of eu-LISA de opgave aankan. Vertraging aan de Europese kant zal de trajecten aan Nederlandse kant beïnvloeden.

Hoewel deze risico's alle drie van buitenaf op de Nederlandse keten afkomen, kunnen de organisaties wel de impact beperken. Door vooruit te denken en tijdig samen af te stemmen.

4.3 Eenmalige opbrengsten en kosten

Zoals beschreven in paragraaf 3.3 is het op dit moment nog niet mogelijk om een berekening te maken van de eenmalige financiële effecten (kosten implementatie), afgezien van een ordening welke posten zwaarder wegen dan anderen. Wel kan dit onderzoek alvast de bovengenoemde effecten ordenen op indicatieve grootte. Een dergelijk getal geeft al een gevoel voor de belangrijkste financiële elementen. De onderstaande tabel bevat de bij de uitvoeringsorganisaties getoetste ordening.

Effect	Toelichting	Orde grootte (éénmalig)
Kosten		
Bijwerken Systemen	**Elke betrokken organisatie moet de gebruikersapplicaties en databases (velden en waarden) van hun systemen bijwerken**	**Miljoenen**
Koppelvlakken	Met de nieuwe componenten ontstaan nieuwe koppelingen. Die worden eenmalig aangelegd, mogelijk per afzonderlijk systeem	Honderd-duizenden
Bijwerken procedures	De werkwijze van de primair processen verandert enigszins. Dit vraagt het herschrijven van processen en verandercommunicatie	Honderd-duizenden
Trainingen	Voorlichting over de toegangsrechten van medewerkers moet nu ook de tweetrapstoegang uitleggen en wordt iets uitgebreider	Honderd-duizenden
Opzetten proces gele links	Het inrichten of uitbreiden van de afdelingen die de gele links uit de MID verwerken, vraagt werving, project- en inrichtingskosten	Honderd-duizenden
Herschrijven autorisatiebeleid	Door de verordeningen moeten organisaties hun autorisatiebeleid herzien. Dit vraagt inzet van gespecialiseerde medewerkers.	Honderd-duizenden
Programmakosten	Nederlandse kosten voor regie, afstemming en coördinatie tussen de betrokkenen over implementatie en achtervangprocedures	Honderd-duizenden
Opbrengsten		
Simpeler EES, ETIAS, ECRIS-TCN	sBMS en CIR leveren componenten die anders voor EES, ETIAS en ECRIS-TCN drie keer apart waren gebouwd en geïmplementeerd	Honderd-duizenden

Al met al vraagt het implementatietraject significante inzet van de uitvoeringsorganisaties. De precieze implementatiekosten hangen af van de vraag welke acties overkoepelend worden uitgevoerd en welke acties door elke organisatie afzonderlijk.

De Europese Commissie stelt naar verwachting €136,3 miljoen beschikbaar voor de implementatiekosten. Dit bedrag moet worden gedeeld door alle lidstaten binnen het EU- en/of Schengengebied en hierbij zijn projectmanagement-, hosting, operatie en communicatiekosten van dit budget uitgesloten. Dat betekent dat niet alle Nederlandse kosten gedekt zullen zijn.

5 Eerstvolgende stappen

In dit hoofdstuk beschrijven we welke besluiten er nog te nemen zijn om de verordeningen goed te kunnen implementeren. Ook leest u wat prioriteit dient te hebben als de uitvoeringsconsequenties verder in beeld worden gebracht.

5.1 Actueel benodigde strategische besluiten

AEF ziet een viertal strategische besluiten die de Nederlandse keten in de komende periode moet nemen:

Wie neemt regie over organisatiegrenzen heen bij de implementatie?
De implementatie van de verordeningen vraagt naar verwachting een aantal acties die over organisatiegrenzen heen bewegen. Zo veranderen er centrale IT-systemen en koppelingen waar meerdere uitvoeringsorganisaties gebruik van maken. Dit vraagt om coördinatie of regie over organisatiegrenzen heen.

Uit de conceptplannen van programma Grenzen en veiligheid blijkt dat dit programma een coördinerende rol gaat vervullen. De verwachting is dat Nederlandse uitvoeringsorganisaties zelf de eindverantwoordelijkheid houden over de implementatie. Zij worden daarbij gefaciliteerd door een vanuit het programma aangestelde implementatiecoördinator. Deze vervult ook een signalerende rol op het moment dat er risico's zijn voor de implementatie.

Organisatieoverschrijdende activiteiten zoals het opstellen van een architectuur en het claimen van financiën bij de Europese fondsen wordt centraal door het programma opgepakt. Over het plan heeft nog geen besluitvorming plaatsgevonden. Deze wordt begin oktober verwacht.

Wie verwerkt de links van meerdere identiteiten?
De Multiple Identity Detector gaat links afgeven dat personen mogelijk meerdere identiteiten gebruiken. Dit zijn de gele links uit hoofdstuk 3. De vraag is hoe deze gele links in de Nederlandse praktijk zullen worden verwerkt.

Enerzijds is het wenselijk dat gele links zo dicht mogelijk bij de bron worden onderzocht en opgespoord, kortom bij medewerkers in het primair proces. Zij hebben de betreffende persoon immers fysiek voor zich staan. Anderzijds is het wenselijk dat er gespecialiseerde kennis is om moeilijke gevallen op te lossen. Dat zou pleiten voor een 'frontoffice' en een 'backoffice'.

Dat roept ten eerste de vraag op wat de taakverdeling tussen front- en backoffice precies wordt en ten tweede wie de rol van backoffice invult. Elke organisatie kan voor zichzelf een eigen backoffice inrichten, maar het kan ook centraal, waar één of enkele afdeling(en) de backofficerol voor de hele Nederlandse keten vervullen.
Op dit moment zijn er in Nederlandse al enkele teams met vergelijkbare taken:

- De Matching Autoriteit van Justid verwerkt nu al gevallen waar aan justitiabelen meer dan één identiteit is toegekend.
- Bureau SIRENE van de Nationale Politie verwerkt signaleringen vanuit het SIS, inclusief signaleringen rond personen met een mogelijke dubbele identiteit.
- Afdeling Dactyloscopie van de Nationale Politie levert diensten voor het herkennen van personen op basis van biometrische kenmerken met behulp van forensische technieken.

Momenteel zijn de betrokkenen nog niet klaar om hier een besluit over te nemen. Uit dit onderzoek komt wel naar voren dat er veel belang wordt gehecht aan de kwaliteit, consistentie en efficiëntie van afhandeling. Dat zou pleiten voor een vorm van centrale verwerking.

Hoe komt het ICT-landschap er aan de Nederlandse kant uit te zien?

In de komende jaren is een nieuwe doelarchitectuur voor het ICT-landschap aan Nederlandse kant nodig. Die verandering ontstaat vanwege de verordeningen van Interoperabiliteit én de andere verordeningen (want die zijn hier niet los van elkaar te zien). Bij het opstellen van een doelarchitectuur gaat een aantal vraagstukken spelen.

Een concreet voorbeeld is dat er slechts enkele verbindingen zijn tussen het web van Nederlandse systemen en het web van Europese systemen. Zo is het enige opstijgpunt tussen de Basisvoorziening vreemdelingen en Europese systemen in beheer bij de Nationale Politie. De Marechaussee heeft voorgesteld dat, nu ze meer op Europese systemen gaat vertrouwen, er een tweede opstijgpunt zou kunnen worden opgezet, dat als achtervang zou kunnen dienen. In het kader van dit onderzoek kan overigens niet worden beoordeeld of dat zinvol is. In elk geval is hiervoor in ieder geval medewerking vanaf de Europese kant nodig.

Hoe, en op welke gronden, worden autorisaties verstrekt?

In het kader van Interoperabiliteit moet het autorisatiebeleid van de uitvoeringsorganisaties worden bijgewerkt. Zoals beschreven in paragraaf 4.2 is er geen totale herziening nodig (de verordeningen willen de toegang stroomlijnen, niet herzien) maar wel een verversing.

In tegenstelling tot de bovenstaande besluiten, kan dit per organisatie worden uitgewerkt, in overleg met de functionarissen gegevensbescherming. Verder is er een link met het Nederlandse beleid- en wetgevingstraject.

Bij de inrichting van de verordeningen gelden de uitgangspunten ‘privacy by design’ en ‘privacy by default’. Dit houdt onder meer in dat elke inrichtingsoptie ook getoetst moet worden aan alle privacyaspecten. De organisaties dienen alleen autorisaties te verlenen wanneer dat wettelijk, noodzakelijk en proportioneel is.

In een interview gaf de Autoriteit Persoonsgegevens aan dat ze groot belang hecht aan een juiste invulling van het autorisatiebeleid. Koppeling van informatiesystemen brengt grotere privacyrisico’s met zich mee. De verwerking biometrische gegevens luistert daarbij extra nauw. De dienst is voornemens om hier nauwgezet monitoringsbeleid op te voeren.

5.2 Inrichting bestuurlijke governance

Een aandachtspunt bij de hiervoor genoemde te nemen besluiten is dat de benodigde bestuurlijke governance nog niet is ingericht op dit brede multidisciplinaire veld. Bij de implementatie zijn ten minste acht uitvoeringsorganisaties betrokken die verantwoording afleggen aan tenminste drie verschillende ministers (JenV, Defensie en Buitenlandse Zaken).[12]

Daarmee overstijgt de implementatie de gebruikelijke gremia. De besluiten kunnen bijvoorbeeld niet alleen binnen het departement van Justitie en Veiligheid worden genomen. Eén van de mogelijkheden die AEF ziet, is dat programma Grenzen en veiligheid het voortouw neemt om deze bestuurlijke governance op te stellen.

Binnen het programma Grenzen en veiligheid kunnen procesafspraken worden gemaakt wie bij welk besluit betrokken wordt. De sponsorgroep, Topberaad+ en/of de programmaraad lijken geschikte gremia om deze afspraken te bekrachtigen.

5.3 Eerste stap richting implementatie

Het implementatietraject van de nieuwe componenten staat op het punt van beginnen. De eerstvolgende stap is om meer technische aspecten uit te werken en met elkaar te bepalen hoe het traject eruitziet. Dit kan met impactanalyses (of gelijksoortige activiteiten).

Op dit moment hebben verschillende organisaties al impactanalyses in voorbereiding. Wij zien een aantal onderwerpen die deze analyses met prioriteit in beeld zouden moeten brengen:

- **Benodigde capaciteit:** in beeld brengen hoeveel capaciteit nodig is voor de eenmalige en structurele effecten en welke kennis en kunde dit vraagt.
- **Precieze toebedeling autorisatierechten:** de impactanalyses zijn een goede aanleiding om verder in beeld te brengen hoe de lees- en schrijfrechten veranderen. Dit kan in overleg met de functionarissen gegevensbescherming van de organisaties.
- **Uitwerken doelarchitectuur:** uitwerken hoe het ICT-landschap eruit komt te zien, voor de organisatie op zichzelf maar ook met ketenpartners. Programma Grenzen en veiligheid is voornemens om de samenwerking tussen ketenpartners te trekken.
- **Gedetailleerder overzicht kostenstructuur:** als uitkomst van (onder andere) deze eerste drie punten zouden de impactanalyses in beeld moeten brengen welke kosten zij gaan maken, in elk geval voor het eenmalige traject, en in hoeverre hier dekking uit Europese middelen voor is.

Analyses per organisatie hoeven zich overigens niet te beperken tot de verordeningen Interoperabiliteit. Het lijkt verstandig om in deze analyses naar het totaalpakket van nieuwe centrale EU-informatiesystemen, geüpdatete systemen en interoperabiliteit te kijken, omdat die zes à zeven verordeningen onderling sterk gerelateerd zijn.

Ook wanneer organisaties nu analyses uitvoeren, duurt het nog enkele jaren voordat de componenten ‘live’ gaan (zie paragraaf 2.2). Dat wil zeggen dat ook deze analyses nog een bepaalde mate van onzekerheid gaan kennen. Later in het traject kan eventueel nog worden besloten om een bijgewerkt beeld op te stellen.

[12] Dat is nog exclusief extra partners als de Douane (Financiën) en de AIVD (BZK).

6 Conclusies

In dit hoofdstuk leest u onze conclusies. De volgorde hiervan volgt de opbouw van dit rapport.

Vertrekpunt (zie hoofdstuk 2)
Nederlandse uitvoeringsorganisaties hebben de verordeningen op de radar en zijn over het algemeen goed op de hoogte van de inhoud van de verordeningen. De grootste organisaties hebben nu projectleiding en -teams of zijn die aan het inrichten om de implementatie vorm te geven.

In de komende tijd (enkele jaren) moeten deze projectteams het nodige werk verrichten om de organisaties op de verordeningen voor te bereiden. Daarom is het van belang dat de individuele organisaties in groter detail beschrijven wat per organisatie benodigd is.

Structurele effecten op primaire processen en bedrijfsvoering (zie hoofdstuk 3)
De verordeningen hebben in het algemeen geen groot effect op de primaire processen van uitvoeringsorganisaties. In Nederland zal de werkwijze van uitvoerende medewerkers niet sterk veranderen; minder dan in andere Europese landen. Dat komt omdat Nederlandse organisaties al functies hebben waarmee ze meerdere registers kunnen doorzoeken. In landen waar dat niet het geval is, bieden de Europese systemen veel meer meerwaarde. De achterliggende Nederlandse bedrijfsvoeringsprocessen veranderen sterker, vooral op het gebied van ICT.

Een uitzondering hierop vormt de Multiple Identity Detector. Daar ontstaat, ook in Nederland, een nieuw proces waarbij signalen rond (misbruik van) meerdere identiteiten automatisch worden afgegeven en structureel worden onderzocht. De uitvoeringsorganisaties verwachten dat dit weliswaar ergens in de keten structureel meer werk vraagt, maar tegelijk een waardevolle bijdrage kan leveren aan bestrijding van georganiseerde criminaliteit, mensenhandel en terrorisme.

Tegenover deze potentiële winst staat een aantal belangrijke risico's. Met interoperabiliteit wordt het toch al complexe ICT-landschap nog complexer en daarmee intensiever om te beheren. Er zijn zorgen over de performance en beschikbaarheid van ICT, die mogelijk kwetsbaarder wordt als die van Europese componenten afhankelijk is. Ten slotte kunnen goedwillende burgers die het slachtoffer zijn van ID-fraude, mogelijk extra hinder ondervinden. Het is nog onzeker of daar voldoende beheersmaatregelen tegen zijn.

Door de componenten voor interoperabiliteit ontstaan in principe geen nieuwe gegevens, dus in dat opzicht gaat Nederland geen nieuwe informatie delen met de rest van Europa.

Eenmalige effecten bij implementatie (zie hoofdstuk 4)

Er is een (eenmalig) implementatietraject nodig om de Interoperabiliteit componenten in de Nederlandse ketenprocessen op te nemen. Uit de scan komt naar voren dat de meerderheid van de inspanningen voor rekening komt van ICT-afdelingen van de verschillende uitvoeringsorganisaties. Zij dienen databases bij te werken en koppelingen aan te passen zodat nationale systemen ook in de toekomst met Europese registers kunnen communiceren. Ook zijn er flinke inspanningen nodig rond instructie en opleiding van medewerkers.

Dit implementatietraject zal niet makkelijk worden. Dat komt omdat het traject voor interoperabiliteit verbonden is met vijf à zes andere trajecten waarbij EU-informatiesystemen worden opgezet of geüpdatet. Uitvoeringsorganisaties waarschuwen dat ze, alles bij elkaar, voor een groot traject staan dat complex wordt om helemaal goed uit te voeren.

In het implementatietraject moet voldoende oog zijn voor het beschermen van persoonsgegevens. De Autoriteit Persoonsgegevens heeft aangegeven dat er daarbij prioriteit moet zijn voor het inrichten van externe security maatregelen en logging functies om ook achteraf te kunnen nagaan wie welke informatie heeft ontsloten.

Eerstvolgende stappen (zie hoofdstuk 5)

Op nationaal niveau zijn er in Nederland nog een aantal strategische besluiten te nemen over de inrichting van het nieuwe ICT-landschap. AEF heeft ten minste vier besluiten geschetst waar in de komende tijd besluitvorming over moet plaatsvinden. De eerste daarvan is wie regie over organisatiegrenzen heen neemt bij implementatie. Van daaruit kunnen de andere punten worden bezien:

- Wie verwerkt de links vanuit de multiple identity detector?
- Hoe komt het ICT-landschap er aan de Nederlandse kant uit te zien?
- Hoe, en op welke gronden, worden autorisaties verstrekt?

In dit vervolgtraject zal samenwerking tussen organisaties (en ook binnen organisaties) van groot belang zijn. In het veld moet dan ook snel een bestuurlijk governancekader worden opgezet waarbinnen deze besluiten genomen kunnen worden.