EUROPESE
COMMISSIE

Straatsburg, 12.12.2017
COM(2017) 794 final

2017/0352 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

tot vaststelling van een kader voor interoperabiliteit tussen de EU-informatiesystemen (politiële en justitiële samenwerking, asiel en migratie)

{SWD(2017) 473} - {SWD(2017) 474}

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

• Achtergrond van het voorstel

De afgelopen drie jaar heeft de EU te maken gekregen met een toenemend aantal irreguliere overschrijdingen van haar buitengrenzen en met een evoluerende en constante bedreiging van de interne veiligheid, getuige een aantal terroristische aanslagen. De EU-burgers rekenen erop dat de personencontrole aan de buitengrens en de controles binnen het Schengengebied doeltreffend zijn, gedegen migratiebeheer mogelijk maken en tot de interne veiligheid bijdragen. Deze uitdagingen hebben eens te meer duidelijk gemaakt dat de informatiemiddelen voor grensbeheer, migratie en veiligheid dringend over de hele linie moeten worden gekoppeld en versterkt.

Informatie kan en moet in de EU doeltreffender en doelmatiger worden beheerd, met volledige inachtneming van de grondrechten, waaronder met name het recht op bescherming van persoonsgegevens, teneinde de buitengrenzen van de EU beter te beschermen, het migratiebeheer te verbeteren en de interne veiligheid voor alle burgers te bevorderen. Er bestaat op EU-niveau al een aantal informatiesystemen om grenswachters, immigratieambtenaren en rechtshandhavingsfunctionarissen van informatie over personen te voorzien, en er worden nog meer van dergelijke systemen ontwikkeld. Wil deze ondersteuning doeltreffend zijn, dan moeten de EU-informatiesystemen informatie verstrekken die volledig, juist en betrouwbaar is. De informatiebeheerstructuur van de EU vertoont echter structurele tekortkomingen. De nationale autoriteiten hebben te maken met een complex landschap van op verschillende manieren beheerde informatiesystemen. Bovendien is de architectuur op het gebied van gegevensbeheer voor grenstoezicht en veiligheid gefragmenteerd, aangezien informatie afzonderlijk wordt opgeslagen in niet-gekoppelde systemen. Dit leidt tot blinde vlekken. Hierdoor zijn **de diverse informatiesystemen op EU-niveau momenteel niet interoperabel** – het is niet mogelijk er gegevens zodanig mee uit te wisselen en te delen dat autoriteiten en bevoegde ambtenaren overal en altijd beschikken over de informatie die zij nodig hebben. Interoperabiliteit van informatiesystemen op EU-niveau kan een aanzienlijke bijdrage leveren tot het wegnemen van de huidige blinde vlekken; vooralsnog kunnen personen namelijk onder verschillende aliassen geregistreerd staan in verschillende, niet-gekoppelde databanken. Daarbij kan het ook gaan om personen die mogelijk bij terroristische activiteiten betrokken zijn.

In april 2016 presenteerde de Commissie een mededeling over **krachtigere en slimmere informatiesystemen voor grenzen en veiligheid**[1] om een aantal structurele tekortkomingen in verband met informatiesystemen aan te pakken[2]. De mededeling van april 2016 had ten doel een discussie op gang te brengen over hoe de informatiesystemen in de Europese Unie het grens- en migratiebeheer en de interne veiligheid krachtiger kunnen bevorderen. De **Raad** heeft van zijn kant eveneens onderkend dat er op dit gebied dringend actie moet worden ondernomen. In juni 2016 heeft de Raad zijn goedkeuring gehecht aan een **routekaart voor het verbeteren van informatie-uitwisseling en informatiebeheer op het gebied van**

[1] COM(2016) 205 van 6 april 2016. .

[2] 1) suboptimale werking van een aantal bestaande informatiesystemen; 2) informatielacunes in de EU-architectuur voor gegevensbeheer; 3) een complex landschap van op verschillende manieren beheerde informatiesystemen; en 4) een gefragmenteerde architectuur op het gebied van gegevensbeheer voor grenstoezicht en veiligheid, waarbij informatie afzonderlijk wordt opgeslagen in onderling niet gekoppelde systemen, wat tot blinde vlekken leidt.

justitie en binnenlandse zaken, onder meer door middel van interoperabiliteitsoplossingen[3]. De routekaart had ten doel operationeel onderzoek te ondersteunen en praktijkmensen (zoals politieambtenaren, grenswachters, officieren van justitie en immigratieambtenaren) van uitgebreide, actuele en hoogwaardige informatie te voorzien, zodat zij doeltreffend kunnen samenwerken en optreden. Ook het **Europees Parlement** heeft aangedrongen op actie op dit gebied. In zijn resolutie van juli 2016[4] over het werkprogramma van de Commissie voor 2017 drong het Europees Parlement aan op *"voorstellen ter verbetering en ontwikkeling van bestaande informatiesystemen, het aanpakken van informatieleemten en de bevordering van interoperabiliteit, en voorstellen voor verplichte gegevensuitwisseling op EU-niveau, samen met de nodige waarborgen voor gegevensbescherming"*. In de Staat van de Unie van september 2016[5] van voorzitter Juncker en in de conclusies van de Europese Raad van december 2016[6] is erop gewezen dat het van groot belang is de tekortkomingen op het gebied van gegevensbeheer te verhelpen en de interoperabiliteit van de informatiesystemen te verbeteren.

In juni 2016 heeft de Commissie naar aanleiding van de mededeling van april 2016 een **deskundigengroep op hoog niveau inzake informatiesystemen en interoperabiliteit**[7] opgericht en deze belast met de aanpak van 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. Het **eindverslag** van deze deskundigengroep op hoog niveau is in mei 2017 gepubliceerd[8]. Het bevat een reeks aanbevelingen om de informatiesystemen van de EU en hun interoperabiliteit te verbeteren. Het Bureau van de Europese Unie voor de grondrechten, de Europese Toezichthouder voor gegevensbescherming en de EU-coördinator voor terrorismebestrijding hebben elk actief deelgenomen aan de werkzaamheden van de deskundigengroep. Elk van deze partijen sprak zijn steun uit, waarbij werd aangetekend dat gaandeweg wel werk dient te worden gemaakt van bredere kwesties op het gebied van grondrechten en gegevensbescherming. Vertegenwoordigers van het secretariaat van de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken van het Europees Parlement en van het secretariaat-generaal van de Raad traden op als waarnemer. De conclusies van de deskundigengroep op hoog niveau waren dat het **noodzakelijk en technisch haalbaar is praktische oplossingen voor interoperabiliteit na te streven**, en dat deze in beginsel zowel operationele voordelen kunnen opleveren als met inachtneming van de voorschriften inzake gegevensbescherming kunnen worden vastgesteld.

Voortbouwend op het verslag en de aanbevelingen van de deskundigengroep presenteerde de Commissie in haar *Zevende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie*[9] een **nieuwe beheersaanpak voor de gegevens** inzake grenzen, veiligheid en migratiebeheer, waarbij alle gecentraliseerde EU-informatiesystemen voor

---

3 Routekaart van 6 juni 2016 voor het verbeteren van informatie-uitwisseling en informatiebeheer op het gebied van justitie en binnenlandse zaken, onder meer door middel van interoperabiliteitsoplossingen — 9368/1/16 REV 1.

4 Resolutie van het Europees Parlement van 6 juli 2016 over de strategische prioriteiten met betrekking tot het werkprogramma van de Commissie voor 2017 (2016/2773(RSP).

5 Staat van de Unie 2016 (14 september 2016): https://ec.europa.eu/commission/state-union-2016_nl.

6 Conclusies van de Europese Raad (15 december 2016), http://data.consilium.europa.eu/doc/document/ST-34-2016-INIT/nl/pdf

7 Besluit van de Commissie van 17 juni 2016 tot oprichting van een deskundigengroep op hoog niveau inzake informatiesystemen en interoperabiliteit – 2016/C 257/03.

8 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

9 COM(2017) 261 final.

veiligheid, grensbeheer en migratiebeheer interoperabel zijn en de grondrechten ten volle worden geëerbiedigd. De Commissie maakte bekend te willen werken aan een Europees zoekportaal waarmee alle relevante EU-systemen op het gebied van veiligheid, grensbeheer en migratiebeheer gelijktijdig kunnen worden doorzocht, eventueel met beter gestroomlijnde regels inzake toegang voor rechtshandhavingsdoeleinden, en voor deze systemen zowel een gezamenlijke dienst voor biometrische matching (eventueel met de mogelijkheid om treffers te markeren[10]) als een gemeenschappelijk identiteitenregister te zullen ontwikkelen. Zij deelde mee zo spoedig mogelijk met een wetgevingsvoorstel inzake interoperabiliteit te zullen komen.

De Europese Raad wees er in zijn conclusies van juni 2017[11] nogmaals op dat optreden geboden was. Voortbouwend op de conclusies van juni 2017[12] van de Raad Justitie en Binnenlandse Zaken verzocht de Europese Raad de Commissie om zo snel mogelijk ontwerpwetgeving op te stellen waarin de aanbevelingen van de deskundigengroep op hoog niveau zijn verwerkt. Met dit initiatief wordt ook gevolg gegeven aan de roep van de Raad om een breed kader voor de toegang voor rechtshandhavingsdoeleinden tot de verschillende databanken op het gebied van justitie en binnenlandse zaken, teneinde meer vereenvoudiging, consistentie, doeltreffendheid en aandacht voor operationele behoeften te verwezenlijken[13]. Ter versterking van de inspanningen om de samenleving van de Europese Unie veiliger te maken, met volledige inachtneming van de grondrechten, kondigde de Commissie in het kader van haar werkprogramma voor 2018[14] aan tegen eind 2017 met een voorstel te zullen komen inzake de interoperabiliteit van informatiesystemen.

- **Doelstellingen van het voorstel**

De algemene doelstellingen van dit initiatief hangen samen met de op het Verdrag gebaseerde doelen om het beheer van de buitengrenzen van het Schengengebied te verbeteren en tot de interne veiligheid van de Europese Unie bij te dragen. Ook vloeien zij voort uit de beleidsbeslissingen van de Commissie en de desbetreffende conclusies van de Europese Raad. Deze doelstellingen worden verder uitgewerkt in de Europese migratieagenda en de daaropvolgende mededelingen, waaronder de mededeling over de instandhouding en de versterking van Schengen[15], de Europese veiligheidsagenda[16] en de werkzaamheden en voortgangsverslagen van de Commissie ter voorbereiding van een echte en doeltreffende veiligheidsunie[17].

---

[10] Een nieuw beginsel van "privacy door ontwerp" dat de toegang tot alle gegevens beperkt tot een "treffer/geen treffer"-melding, d.w.z. uitsluitsel of er al dan niet gegevens beschikbaar zijn.

[11] Conclusies van de Europese Raad, 22-23 juni 2017.

[12] Resultaten van de 3546e zitting van de Raad Justitie en Binnenlandse Zaken van 8 en 9 juni 2017, 10136/17.

[13] Het Comité van permanente vertegenwoordigers (Coreper) van de Raad gaf het voorzitterschap van de Raad op 2 maart 2017 een mandaat om interinstitutionele onderhandelingen te voeren over het EU-inreis-uitreissysteem; aansluitend nam het een ontwerpverklaring van de Raad aan waarbij de Commissie werd verzocht een voorstel in te dienen voor een breed kader voor de toegang voor rechtshandhavingsdoeleinden tot de verschillende databanken op het gebied van justitie en binnenlandse zaken, teneinde te komen tot een sterkere vereenvoudiging, een sterkere samenhang en doeltreffendheid en meer aandacht voor de operationele behoeften (beknopt verslag 7177/17 van 21.3.2017).

[14] COM(2017) 650 final.

[15] COM(2017) 570 final.

[16] COM(2015) 185 final.

[17] COM(2016) 230 final.

Ofschoon de doelstellingen van dit voorstel met name uit de mededeling van april 2016 en de bevindingen van de deskundigengroep op hoog niveau voortvloeien, hangen zij intrinsiek samen met voornoemde teksten.

De specifieke doelstellingen van dit voorstel zijn:

(1) waarborgen dat eindgebruikers (met name grenswachters, rechtshandhavingsambtenaren, immigratiefunctionarissen en gerechtelijke autoriteiten) **snelle, naadloze, systematische en gecontroleerde toegang** hebben tot de informatie die zij nodig hebben om hun taken te verrichten;

(2) zorgen voor een oplossing voor het **opsporen van gevallen waarin meerdere identiteiten** gelinkt zijn aan dezelfde reeks biometrische gegevens, met als dubbel oogmerk enerzijds bonafide personen correct te identificeren en anderzijds **identiteitsfraude te bestrijden**;

(3) het gemakkelijker maken voor politiediensten om de **identiteit te controleren van onderdanen van derde landen** die zich op het grondgebied van een lidstaat bevinden. alsmede

(4) vergemakkelijken en stroomlijnen van de **toegang van rechtshandhavingsinstanties** tot niet voor rechtshandhaving bedoelde informatiesystemen op EU-niveau, waar dit nodig is voor preventie, opsporing, onderzoek of vervolging van zware criminaliteit en terrorisme.

Naast deze primaire operationele doelstellingen zal dit voorstel ook bijdragen tot:

- het vergemakkelijken van de technische en operationele **implementatie** van bestaande en toekomstige (nieuwe) informatiesystemen **door de lidstaten**;
- het versterken en stroomlijnen van de **voorwaarden inzake gegevensbeveiliging en -bescherming** voor de respectieve systemen: alsmede
- het verbeteren en harmoniseren van de vereisten inzake de **gegevenskwaliteit** van de respectieve systemen.

Ten slotte bevat dit voorstel voorschriften inzake het vaststellen en beheren van het Universal Message Format (UMF) als EU-standaard voor de ontwikkeling van informatiesystemen op het gebied van justitie en binnenlandse zaken, en inzake het instellen van een centraal register voor rapportage en statistieken.

- **Toepassingsgebied van het voorstel**

Net als het bijbehorende, op dezelfde datum gepresenteerde voorstel heeft dit voorstel inzake interoperabiliteit betrekking op de op centraal niveau geëxploiteerde EU-informatiesystemen voor veiligheid, grensbeheer en migratiebeheer. Van deze systemen bestaan er al drie. Daarnaast is er een systeem dat zeer binnenkort wordt ontwikkeld en voor nog twee andere systemen zijn voorstellen ingediend die de medewetgevers momenteel bespreken. Elk systeem heeft zijn eigen doelstellingen, doelen, rechtsgrondslagen, regels, gebruikers en institutionele context.

De drie reeds bestaande gecentraliseerde informatiesystemen zijn:

- het **Schengeninformatiesysteem (SIS)**, met een breed spectrum van signaleringen inzake personen (weigeringen van toegang of verblijf, Europees aanhoudingsbevel, vermissingen, rechtshulp, onopvallende en gerichte controles) en voorwerpen (onder meer verloren, gestolen en ongeldig gemaakte identiteitsbewijzen of reisdocumenten)[18].
- het **Eurodac**-systeem met vingerafdrukken van asielzoekers en onderdanen van derde landen die de buitengrens irregulier hebben overschreden of illegaal in een lidstaat verblijven; en
- het **Visuminformatiesysteem (VIS)** met gegevens over visa voor kort verblijf.

Naast deze bestaande systemen heeft de Commissie in 2016-2017 drie nieuwe gecentraliseerde EU-informatiesystemen voorgesteld:

- het **inreis-uitreissysteem (EES)**, waarvoor onlangs de rechtsgrondslag is vastgesteld en dat in de plaats zal komen van het huidige systeem waarbij paspoorten handmatig worden afgestempeld. In het EES zal automatisch een registratie worden opgenomen van de naam, het soort reisdocument, biometrische gegevens en de datum en plaats van inreis en uitreis van onderdanen van derde landen die het Schengengebied voor een kort verblijf bezoeken;
- het voorgestelde **Europees systeem voor reisinformatie en -autorisatie (ETIAS)**, dat – eenmaal vastgesteld – grotendeels automatisch de informatie moet verzamelen en controleren die niet-visumplichtige onderdanen van derde landen voorafgaand aan hun reis naar het Schengengebied opgeven; en
- het voorgestelde **Europees Strafregister Informatiesysteem voor onderdanen van derde landen (ECRIS-TCN)**, een elektronisch systeem voor de uitwisseling van informatie over eerdere veroordelingen van onderdanen van derde landen door de strafrechter in de EU.

Deze zes systemen zijn complementair en — met uitzondering van het SIS — uitsluitend gericht op onderdanen van derde landen. De systemen ondersteunen de nationale autoriteiten bij het grens-, migratie-, visum- en asielbeheer en bij de bestrijding van criminaliteit en terrorisme. Dit geldt met name voor het SIS, momenteel het meest gebruikte instrument voor informatie-uitwisseling in het kader van rechtshandhaving.

Naast deze centraal, op EU-niveau, beheerde informatiesystemen omvat het toepassingsgebied van dit voorstel ook de **Interpol**-databank voor verloren en gestolen reisdocumenten (SLTD), die krachtens de Schengengrenscode stelselmatig wordt doorzocht aan de buitengrenzen van de EU, en de Interpol-databank voor reisdocumenten met signaleringen (TDAWN). Dit initiatief heeft ook betrekking op gegevens van **Europol**, voor zover deze van belang zijn voor de werking van het voorgestelde ETIAS-systeem en voor het assisteren van de lidstaten bij het zoeken naar gegevens over zware criminaliteit en terrorisme.

[18] In de ontwerpverordeningen betreffende het SIS die de Commissie in december 2016 heeft gepresenteerd, wordt voorgesteld om hier terugkeerbesluiten en ondervragingscontroles aan toe te voegen.

Nationale informatiesystemen en gedecentraliseerde EU-informatiesystemen vallen buiten het toepassingsgebied van dit initiatief. Mits wordt aangetoond dat zulks noodzakelijk is, kunnen gedecentraliseerde systemen zoals de instrumenten die worden beheerd krachtens het Prümkader[19], de richtlijn over het gebruik van persoonsgegevens van passagiers(PNR)[20] en de richtlijn betreffende persoonsgegevens van passagiers[21] in een latere fase worden gekoppeld aan een of meer van de uit hoofde van dit initiatief voorgestelde componenten[22].

Om het onderscheid in acht te nemen tussen enerzijds zaken die een ontwikkeling vormen van het Schengenacquis inzake grenzen en visa en anderzijds systemen die betrekking hebben op het Schengenacquis inzake politiesamenwerking of losstaan van het Schengenacquis, wordt in dit voorstel de toegang tot het Schengeninformatiesysteem zoals momenteel geregeld door Besluit 2007/533/JBZ, behandeld, alsook Eurodac en [het ECRIS-TCN].

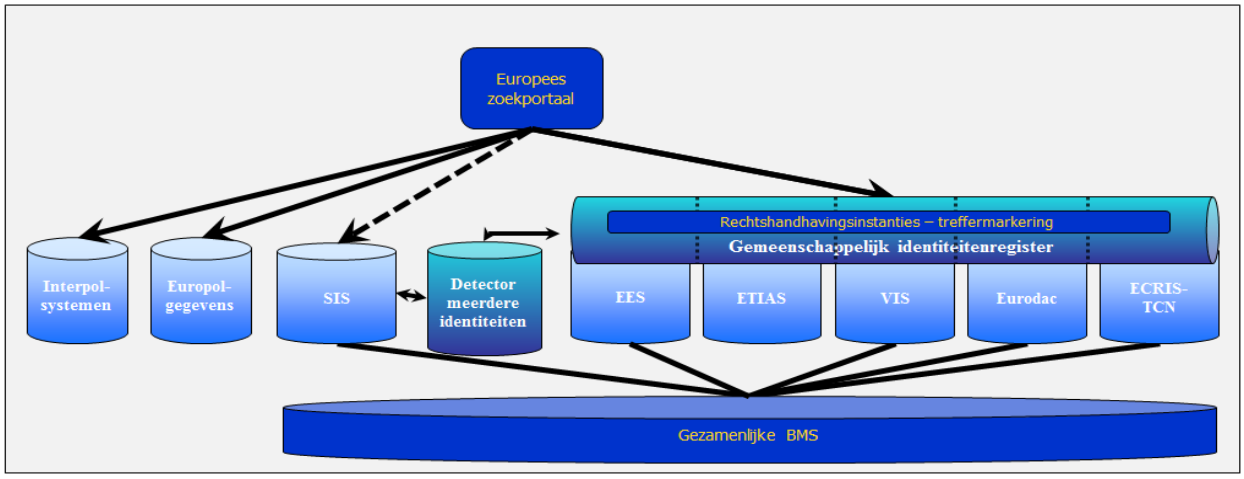
- **Technische componenten die nodig zijn om interoperabiliteit te verwezenlijken**

Om de doelstellingen van dit voorstel te bereiken, moeten met het oog op interoperabiliteit vier componenten tot stand worden gebracht:

- Europees zoekportaal (*European search portal* — ESP)
- Gezamenlijke dienst voor biometrische matching (*biometric matching service* — BMS)
- Gemeenschappelijk identiteitenregister (*common identity repository* — CIR)
- Detector van meerdere identiteiten (*multiple-identity detector* — MID)

Deze componenten worden elk uitvoerig beschreven in het werkdocument van de diensten van de Commissie over de effectbeoordeling bij dit voorstel.

De vier componenten vormen samen de volgende interoperabiliteitsoplossing:



[19] http://eur-lex.europa.eu/legal-content/NL/TXT/?qid=1508936184412&uri=CELEX:32008D06 15.
[20] http://eur-lex.europa.eu/legal-content/NL/TXT/?qid=1508936384641&uri=CELEX:32016L06 81.
[21] Richtlijn 2004/82/EG van de Raad van 29 april 2004 betreffende de verplichting voor vervoerders om passagiersgegevens door te geven.
[22] Evenzo verzocht de Raad de Commissie in zijn conclusies van juni 2017 een haalbaarheidsstudie te ondernemen om de technische, operationele en juridische aspecten van de interoperabiliteit van de beveiligings- en grensbeheersystemen met de douanesystemen verder te onderzoeken, en haar bevindingen uiterlijk eind 2018 ter bespreking aan de Raad voor te leggen.

De doelstellingen en werking van deze vier componenten kunnen als volgt worden samengevat:

(1) Het **Europees zoekportaal (ESP)** moet het mogelijk maken om gelijktijdig meerdere systemen (het centrale SIS, Eurodac, het VIS, het toekomstige EES, de voorgestelde systemen ETIAS en ECRIS-TCN, alsmede de relevante systemen van Interpol en gegevens van Europol), te doorzoeken aan de hand van identiteitsgegevens (zowel biografische als biometrische gegevens). Hierdoor zouden gebruikers van de EU-informatiesystemen snel, naadloos, doeltreffend, systematisch en gecontroleerd toegang krijgen tot alle informatie die zij nodig hebben om hun taken te verrichten.

Een zoekopdracht via het Europees zoekportaal moet in slechts enkele seconden, informatie opleveren uit de diverse systemen waartoe de gebruiker rechtens toegang heeft. Afhankelijk van het doel van de zoekopdracht en de overeenkomstige toegangsrechten moet het ESP specifiek worden geconfigureerd.

Het is niet de bedoeling dat het ESP nieuwe gegevens verwerkt of gegevens opslaat; het moet louter dienstdoen als één loket of "messagebroker" voor het doorzoeken van verscheidene centrale systemen en voor het naadloos opzoeken van de nodige informatie. De voorschriften inzake toegangscontrole en gegevensbescherming van de onderliggende systemen zouden hierbij ten volle worden geëerbiedigd. Met het ESP moet het eenvoudiger worden om elk van de bestaande EU-informatiesystemen op de juiste en toegestane wijze te benutten en moet het gemakkelijker en goedkoper worden voor de lidstaten om de systemen te raadplegen en gebruiken overeenkomstig de rechtsinstrumenten die daarop van toepassing zijn.

(2) De **gezamenlijke dienst voor biometrische matching (gezamenlijke BMS)** moet het mogelijk maken om biometrische gegevens (vingerafdrukken en gezichtsopnames) te doorzoeken en te vergelijken vanuit meerdere centrale systemen (met name het SIS, Eurodac, het VIS, het toekomstige EES en het voorgestelde ECRIS-TCN). Het voorgestelde ETIAS zal geen biometrische gegevens bevatten en het zal dan ook niet worden gekoppeld aan de gezamenlijke BMS.

Waar elk centraal systeem (het SIS, Eurodac, het VIS) momenteel met een specifieke propriëtaire zoekmachine voor biometrische gegevens werkt[23], zou een gezamenlijke dienst voor biometrische matching fungeren als een gezamenlijk platform waarop de gegevens gelijktijdig worden doorzocht en vergeleken. De gezamenlijke BMS moet aanzienlijke voordelen qua veiligheid, kosten, onderhoud en beheer opleveren door te werken met één enkele technologische component, in plaats van met vijf verschillende. De biometrische gegevens (vingerafdrukken en gezichtsopnames) worden uitsluitend bewaard in de onderliggende systemen. De gezamenlijke BMS moet een mathematische representatie van de biometrische informatie (een template) genereren en bewaren, maar de eigenlijke gegevens buiten beschouwing laten; deze gegevens worden dus slechts eenmaal, op één locatie, opgeslagen.

[23] Deze biometrische zoekmachines worden technisch aangeduid als geautomatiseerd identificatiesysteem voor vingerafdrukken (AFIS) of als geautomatiseerd biometrisch identificatiesysteem (ABIS).

De gezamenlijke BMS zou het een stuk gemakkelijker maken om verbanden te ontdekken tussen gegevensreeksen en de meerdere identiteiten waaronder één en dezelfde persoon in verschillende centrale systemen bekendstaat. Zonder een gezamenlijke BMS fungeert geen van de andere drie componenten.

3) Het **gemeenschappelijke identiteitenregister (CIR)** moet fungeren als de gezamenlijke component voor het bewaren van biografische[24] en biometrische identiteitsgegevens van onderdanen van derde landen die zijn opgeslagen in Eurodac, het VIS, het toekomstige EES, het voorgestelde ETIAS en het voorgestelde ECRIS-TCN. Elk van deze vijf centrale systemen legt om specifieke redenen biografische gegevens over specifieke personen vast. Daarin zou geen verandering komen. De relevante identiteitsgegevens zouden worden bewaard in het CIR, maar moeten deel blijven uitmaken van de onderliggende systemen waarin deze gegevens zijn geregistreerd.

Het CIR zou geen SIS-gegevens bevatten. Door de complexe technische architectuur van SIS – met nationale kopieën, gedeeltelijke nationale kopieën en eventuele nationale systemen voor biometrische matching – zou het CIR zo complex worden dat het technisch en financieel onuitvoerbaar wordt.

Het CIR moet het in de eerste plaats gemakkelijker maken een onderdaan van een derde land te identificeren. Dit zou operaties sneller doen verlopen, de doelmatigheid verbeteren en schaalvoordelen opleveren. De totstandbrenging van het CIR is nodig om de identiteit van onderdanen van derde landen doeltreffend te kunnen controleren, ook op het grondgebied van een lidstaat. Door aan het CIR de mogelijkheid toe te voegen om treffers te markeren, moet het mogelijk worden om aan de hand van een eenvoudige "treffer/geen treffer"-melding na te gaan of gegevens al dan niet voorkomen in een of meer van de door het CIR bestreken systemen. Zo zou het CIR ook helpen om de toegang van rechtshandhavingsinstanties tot niet voor rechtshandhaving bedoelde informatiesystemen te stroomlijnen en tegelijk de gegevensbescherming krachtig te blijven waarborgen (zie het onderstaande deel over de tweefasenaanpak van de toegang voor rechtshandhaving).

Van de vijf systemen die het CIR zou moeten bestrijken, zijn het toekomstige EES, het voorgestelde ETIAS en het voorgestelde ECRIS-TCN nieuw; deze systemen moeten nog worden ontwikkeld. Het huidige Eurodac bevat geen biografische gegevens; hiervoor wordt een uitbreiding ontwikkeld wanneer de nieuwe rechtsgrondslag voor Eurodac eenmaal is vastgesteld. Het huidige VIS bevat geen biografische gegevens, maar de nodige interacties tussen het VIS en het toekomstige EES nopen tot modernisering van het VIS in zijn huidige vorm. De totstandbrenging van het CIR zou dan ook op het juiste moment komen. Het CIR zou bestaande gegevens op geen enkele manier dupliceren. Technisch zou het CIR worden ontwikkeld op basis van het EES/ETIAS-platform.

4) De **detector van meerdere identiteiten (MID)** moet controleren of de gezochte identiteitsgegevens voorkomen in meer dan één van de aan de detector gekoppelde systemen. De MID bestrijkt de systemen die identiteitsgegevens in het CIR opslaan (Eurodac, het VIS, het toekomstige EES, het voorgestelde ETIAS en het voorgestelde ECRIS-TCN) en het SIS. De MID moet het mogelijk maken gevallen op te sporen waarin

[24] Op het reisdocument staan onder meer de volgende biografische gegevens: achternaam, voornaam, geslacht, geboortedatum, nummer van reisdocument. Reisdocumenten vermelden geen adressen, vroegere namen, biometrische gegevens enz.

meerdere identiteiten gelinkt zijn aan dezelfde reeks biometrische gegevens, met als dubbel oogmerk enerzijds bonafide personen correct te identificeren en anderzijds identiteitsfraude te bestrijden.

Dankzij de MID zou kunnen worden vastgesteld dat verschillende namen betrekking hebben op dezelfde identiteit. Deze innovatie is noodzakelijk voor een doeltreffende aanpak van het frauduleuze gebruik van identiteiten, dat een ernstige inbreuk op de veiligheid vormt. Het is de bedoeling dat de MID alleen de biografische identiteitsgegevens weergeeft waarnaar in meerdere centrale systemen wordt gelinkt. Deze links moeten worden ontdekt door gebruik te maken van de gezamenlijke dienst voor biometrische matching en zouden moeten worden bevestigd of terzijde geschoven door de instantie die de gegevens heeft opgeslagen in het informatiesysteem van waaruit de link is gelegd. Om de bevoegde gebruikers van de MID bij deze taak te ondersteunen, zou het systeem de geïdentificeerde links in vier categorieën moeten onderverdelen:

- gele link – mogelijk verschillende biografische identiteiten van dezelfde persoon
- witte link – bevestiging dat de verschillende biografische identiteiten van een en dezelfde bonafide persoon zijn
- groene link – bevestiging dat verschillende bonafide personen toevallig dezelfde biografische identiteit delen
- rode link – vermoeden dat één persoon onwettig gebruikmaakt van verschillende biografische identiteiten.

Dit voorstel beschrijft de procedures die zouden moeten worden ingevoerd om met deze verschillende categorieën om te gaan. Er dient zo snel mogelijk uitsluitsel te worden geboden over de identiteit van de betrokken bonafide personen, door de gele link om te zetten in een bevestigde groene of witte link, teneinde onnodige hinder te voorkomen. Waar de beoordeling echter uitwijst dat er inderdaad sprake is van een rode link of dat een gele link moet worden veranderd in een rode link, zou passende actie moeten worden ondernomen.

- **De tweefasenaanpak van de toegang voor rechtshandhavingsinstanties via het gemeenschappelijk identiteitenregister**

Rechtshandhaving is een secundaire of nevendoelstelling van Eurodac, het VIS, het toekomstige EES en het voorgestelde ETIAS. De mogelijkheden om toegang tot de in deze systemen opgeslagen gegevens te krijgen voor rechtshandhavingsdoeleinden zijn dan ook beperkt. Rechtshandhavingsinstanties mogen deze niet voor rechtshandhaving bedoelde informatiesystemen alleen raadplegen met het oog op preventie, opsporing, onderzoek of vervolging van terrorisme en andere vormen van zware criminaliteit. Bovendien lopen de toegangsvoorwaarden en waarborgen voor de verschillende systemen uiteen en zouden sommige van de huidige regels de snelheid van het rechtmatig gebruik door deze instanties kunnen drukken. Meer algemeen beperkt het beginsel dat eerst in nationale databanken moet worden gezocht de mogelijkheden van de autoriteiten van de lidstaten om systemen te raadplegen voor rechtmatige rechtshandhavingsdoeleinden, waardoor kansen om benodigde informatie boven water te krijgen, wellicht onbenut blijven.

In haar mededeling van april 2016 onderkende de Commissie dat de bestaande instrumenten voor rechtshandhavingsdoeleinden dienen te worden geoptimaliseerd, met inachtneming van de gegevensbeschermingsvoorschriften. Deze zienswijze werd bevestigd en nogmaals tot uitdrukking gebracht door de lidstaten en de relevante agentschappen in het kader van de deskundigengroep op hoog niveau.

Door de totstandbrenging van het CIR, waarmee treffers kunnen worden gesignaleerd, voorziet dit voorstel derhalve in de mogelijkheid om het EES, het VIS, het ETIAS en Eurodac door middel van een **tweefasenaanpak te raadplegen**. Deze tweefasenaanpak zou onverlet laten dat rechtshandhaving louter een nevendoelstelling van deze systemen is en dat er voor de toegang voor rechtshandhavingsdoeleinden strikte voorwaarden moeten gelden.

Eerst zou een rechtshandhavingsambtenaar een zoekopdracht betreffende een specifiek persoon uitvoeren op basis van diens identiteitsgegevens, reisdocument of biometrische gegevens, om na te gaan of er informatie over de gezochte persoon is opgeslagen in het CIR. Als dergelijke gegevens aanwezig zijn, ontvangt de ambtenaar een **antwoord waaruit blijkt welk(e) van de EU-informatiesystemen informatie** over de betrokkene bevat(ten) (**treffermarkering**). De ambtenaar zou geen toegang tot gegevens in de onderliggende systemen krijgen.

In tweede instantie zou de ambtenaar kunnen vragen om toegang tot elk afzonderlijk systeem waarvan is bericht dat het gegevens bevat, teneinde het volledige dossier te verkrijgen over de persoon op wie de zoekopdracht betrekking had, **overeenkomstig de bestaande regels en procedures die voor elk van de betrokken systemen gelden**. Bij deze tweede stap zouden voor toegang nog steeds voorafgaande toestemming van een bevoegde autoriteit alsmede een specifieke user-ID en registratie in logbestanden vereist zijn.

Deze nieuwe benadering zou ook een meerwaarde hebben voor de rechtshandhavingsinstanties, door het **bestaan van potentiële links** in de MID. De MID zou het CIR helpen om bestaande links te identificeren, waardoor de zoekopdracht nog aan nauwkeurigheid wint. De MID zou kunnen aangeven of de persoon in verschillende informatiesystemen **onder verschillende identiteiten bekendstaat**.

De tweefasenaanpak inzake gegevensraadpleging is met name van belang voor zaken waarin de verdachte, de dader of het mogelijke slachtoffer van een terroristisch misdrijf of ander ernstig strafbaar feit **onbekend is**. In dergelijke gevallen zou het CIR met een enkele zoekopdracht het informatiesysteem kunnen identificeren waarin de betrokkene is opgenomen. Hierdoor worden de huidige voorwaarden dat eerst in de nationale databanken en vervolgens in het geautomatiseerd identificatiesysteem voor vingerafdrukken van andere lidstaten krachtens Besluit 2008/615/JBZ (“Prümcontrole”) moet worden gezocht, overbodig.

De nieuwe tweefasenaanpak inzake raadpleging zou pas **van kracht moeten worden** wanneer de nodige **interoperabiliteitscomponenten volledig operationeel** zijn.

- **Aanvullende elementen van dit voorstel ter ondersteuning van de interoperabiliteitscomponenten/onderdelen**

1) Naast de bovenstaande componenten bevat deze ontwerpverordening ook het voorstel om een **centraal register voor rapportage en statistieken (CRRS) op te zetten**. Dit register is nodig om verslagen met (anonieme) statistische gegevens samen te stellen en te delen

voor operationele, beleids- en gegevenskwaliteitsdoeleinden. De huidige praktijk waarbij statistische informatie alleen op de afzonderlijke informatiesystemen wordt verzameld, is ongunstig voor de gegevensbeveiliging en prestaties. Bovendien is het hierdoor niet mogelijk dwarsverbanden te leggen tussen gegevens in verschillende systemen.

Het CRRS moet dienen als een speciaal, afzonderlijk register voor geanonimiseerde statistische gegevens die ontleend zijn aan het SIS, het VIS, Eurodac, het toekomstige EES, het voorgestelde ETIAS, het voorgestelde ECRIS-TCN, het gemeenschappelijke identiteitenregister, de detector van meerdere identiteiten en de gezamenlijke dienst voor biometrische matching. Het register moet de mogelijkheid bieden om verslagen op beveiligde wijze te delen (conform de voorschriften van de respectieve rechtsinstrumenten) met de lidstaten, de Commissie (met inbegrip van Eurostat) en EU-agentschappen.

Het is goedkoper om één centraal register te ontwikkelen in plaats van afzonderlijke registers voor elk systeem, en de totstandkoming, het beheer en het onderhoud ervan zouden minder inspanningen vergen. Ook de gegevensbeveiliging zou erdoor verbeteren, aangezien de gegevensopslag en de toegangscontrole zich beperken tot één register.

2) In deze ontwerpverordening wordt ook voorgesteld om een **Universal Message Format (UMF)** vast te stellen als de standaard die op EU-niveau moet worden gebruikt om op interoperabele wijze de interactie tussen meerdere systemen – waaronder de door eu-LISA ontwikkelde en beheerde systemen – in goede banen te leiden. Het gebruik van de standaard door Europol en Interpol zou ook worden aangemoedigd.

Met de UMF-standaard worden gemeenschappelijke uniforme formuleringen ingevoerd voor het beschrijven en linken van gegevenselementen, en met name de elementen die betrekking hebben op personen en (reis)documenten. Het gebruik van het UMF bij de ontwikkeling van nieuwe informatiesystemen vereenvoudigt de integratie en interoperabiliteit met andere systemen, met name voor lidstaten die interfaces moeten bouwen om met deze nieuwe systemen te communiceren. Wat dat betreft kan het verplichte gebruik van het UMF bij de ontwikkeling van nieuwe systemen worden beschouwd als een noodzakelijke randvoorwaarde voor de invoering van de in deze verordening voorgestelde interoperabiliteitscomponenten.

Om ervoor te zorgen dat de UMF-standaard in de hele EU volledig wordt ingevoerd, wordt een passende beheerstructuur voorgesteld. Het zou de taak zijn van de Commissie om de UMF-standaard vast te stellen en te ontwikkelen, in het kader van een onderzoeksprocedure met de lidstaten. De geassocieerde Schengenlanden, de EU-agentschappen en de internationale organen die bij de UMF-projecten betrokken zijn (zoals eu-LISA, Europol en Interpol), zullen hier ook bij worden betrokken. De voorgestelde beheerstructuur is van vitaal belang om het UMF brede ingang te doen vinden en daarbij optimale bruikbaarheid en toepasbaarheid te waarborgen.

3) Bij deze ontwerpverordening worden bovendien **geautomatiseerde mechanismen voor de controle van gegevenskwaliteit** en gemeenschappelijke indicatoren voor gegevenskwaliteit ingevoerd; ook worden de lidstaten ertoe verplicht om bij het invoeren van gegevens in de systemen en het gebruik van die systemen een optimale gegevenskwaliteit te waarborgen. Als de gegevenskwaliteit niet optimaal is, kan dat niet alleen gevolgen hebben doordat gezochte personen niet kunnen worden geïdentificeerd,

maar kunnen ook de grondrechten van onschuldige mensen worden aangetast. Om de problemen te verhelpen die zouden kunnen voortvloeien uit de door menselijke gebruikers ingevoerde gegevens, zouden bepalingen inzake automatische validering kunnen voorkomen dat operatoren fouten maken. Daarbij zou het streven erop gericht zijn kennelijk onjuiste of inconsistente gegevensinvoer automatisch te herkennen, zodat de lidstaat die de gegevens heeft ingevoerd, deze kan verifiëren en zo nodig corrigerende maatregelen kan nemen. Ter aanvulling hiervan zou eu-LISA regelmatig verslag kunnen uitbrengen over de gegevenskwaliteit.

- **Consequenties voor andere rechtsinstrumenten**

Deze ontwerpverordening en het bijbehorende voorstel omvatten innovaties die nopen tot wijziging van andere rechtsinstrumenten:

- Verordening (EU) 2016/399 (Schengengrenscode)
- Verordening (EU) 2017/2226 (EES-verordening)
- Verordening (EU) nr. 767/2008 (VIS-verordening)
- Beschikking 2004/512/EG van de Raad (VIS-beschikking)
- Besluit 2008/633/JBZ van de Raad (besluit over VIS/toegang voor rechtshandhavingsdoeleinden)
- [ETIAS-verordening]
- [Eurodac-verordening]
- [SIS-verordeningen]
- [ECRIS-TCN-verordening, met inbegrip van de overeenkomstige bepalingen van Verordening (EU) 2016/1624 (verordening betreffende de Europese grens- en kustwacht)]
- [eu-LISA-verordening]

Zowel het onderhavige als het bijbehorende voorstel bevat gedetailleerde bepalingen inzake de veranderingen die moeten worden aangebracht in de rechtsinstrumenten waarvoor de medewetgevers stabiele voorschriften hebben vastgesteld: de Schengengrenscode, de EES-verordening, de VIS-verordening, Besluit 2008/633/JBZ van de Raad en Beschikking 2004/512/EG van de Raad.

Over de overige vermelde instrumenten (verordeningen inzake het ETIAS, Eurodac, het SIS, ECRIS-TCN en eu-LISA) wordt momenteel onderhandeld in het Europees Parlement en de Raad. Vooralsnog kunnen de wijzigingen die nodig zijn voor deze instrumenten derhalve niet worden vastgesteld. De Commissie zal dergelijke wijzigingen voor elk van deze instrumenten presenteren binnen twee weken nadat over de respectieve ontwerpverordeningen een politiek akkoord is bereikt.

- **Verenigbaarheid met bestaande bepalingen op het beleidsterrein**

Dit voorstel maakt deel uit van een breder proces waartoe de aanzet is gegeven met de mededeling van april 2016 over krachtigere en slimmere informatiesystemen voor grenzen en veiligheid, en met de daaropvolgende werkzaamheden van de deskundigengroep op hoog niveau inzake informatiesystemen en interoperabiliteit. Het voorstel heeft drie doelstellingen:

a) de voordelen van de **bestaande informatiesystemen** versterken en optimaliseren;

b) informatielacunes aanpakken door nieuwe informatiesystemen op te zetten;

c) de interoperabiliteit van deze systemen versterken.

Voor de eerste doelstellingen heeft de Commissie in december 2016 voorstellen goedgekeurd met het oog op de verdere verbetering van het huidige Schengeninformatiesysteem (SIS)[25]. Wat Eurodac betreft, zijn na het voorstel van de Commissie van mei 2016[26] de onderhandelingen over de herziene rechtsgrondslag versneld. Ook wordt er gewerkt aan een voorstel voor een nieuwe rechtsgrondslag voor het Visuminformatiesysteem (VIS), dat in het tweede kwartaal van 2018 zal worden ingediend.

Voor de tweede doelstelling zijn al in juli 2017 onderhandelingen afgerond in verband met het voorstel van de Commissie van april 2016 tot instelling van een inreis-uitreissysteem (EES)[27]. De medewetgevers hebben toen een politiek akkoord bereikt, dat in oktober 2017 is bevestigd door het Europees Parlement en in november 2017 formeel is aangenomen door de Raad. De rechtsgrondslag wordt in december 2017 van kracht. De onderhandelingen over het voorstel van november 2016 tot instelling van een Europees systeem voor reisinformatie en -autorisatie (ETIAS)[28] zijn begonnen en zullen naar verwachting in de komende maanden worden afgerond. In juni 2017 heeft de Commissie een rechtsgrondslag voorgesteld voor de aanpak van een andere informatielacune: het Europees Strafregister Informatiesysteem voor onderdanen van derde landen (ECRIS-TCN)[29]. Ook in dit geval hebben de medewetgevers verklaard te streven naar een spoedige vaststelling van deze rechtsgrondslag.

Het huidige voorstel betreft de derde doelstelling die in de mededeling van april 2016 is geformuleerd.

- **Samenhang met ander beleid van de Unie op het gebied van justitie en binnenlandse zaken**

Het onderhavige en het bijbehorende voorstel vloeien voort uit en stroken met de Europese migratieagenda en navolgende mededelingen, waaronder de mededeling over de instandhouding en de versterking van Schengen[30], alsook met de Europese veiligheidsagenda[31] en het werk en de voortgangsverslagen van de Commissie ter voorbereiding van een echte en doeltreffende veiligheidsunie[32]. Dit voorstel is in overeenstemming met ander beleid van de Unie, met name op het gebied van:

- Interne veiligheid: volgens de Europese veiligheidsagenda zijn strenge gemeenschappelijke normen voor grensbeheer essentieel om grensoverschrijdende criminaliteit en terrorisme te voorkomen. Dit voorstel draagt verder bij tot een hoge mate van interne veiligheid door de middelen aan te reiken die autoriteiten snelle, naadloze, systematische en gecontroleerde toegang bieden tot de informatie die zij nodig hebben.

[25] COM(2016) 883 final.
[26] COM(2016) 272 final.
[27] COM(2016) 194 final.
[28] COM(2016) 731 final.
[29] COM(2017) 344 final.
[30] COM(2017) 570 final.
[31] COM(2015) 185 final.
[32] COM(2016) 230 final.

- Asiel: het voorstel merkt Eurodac aan als een van de centrale EU-systemen die interoperabel moeten worden gemaakt.
- Buitengrensbeheer en veiligheid: dit voorstel versterkt het SIS en het VIS, die bijdragen tot de doeltreffende controle van de buitengrenzen van de Unie, alsook het toekomstige EES, het voorgestelde ETIAS en het voorgestelde ECRIS-TCN.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

• Rechtsgrondslag

De belangrijkste rechtsgrondslag wordt gevormd door de volgende artikelen van het Verdrag betreffende de werking van de Europese Unie: Artikel 16, lid 2, artikel 74, artikel 78, lid 2, onder e), artikel 79, lid 2, onder c), artikel 82, lid 1, onder d), artikel 85, lid 1, artikel 87, lid 2, onder a), en artikel 88, lid 2.

Krachtens artikel 16, lid 2, VWEU beschikt de Unie over de bevoegdheid om voorschriften vast te stellen betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie, alsook door de lidstaten, bij de uitoefening van activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, alsmede de voorschriften betreffende het vrij verkeer van die gegevens. Krachtens artikel 74 kan de Raad maatregelen vaststellen voor de administratieve samenwerking tussen de diensten van de lidstaten in de ruimte van vrijheid, veiligheid en recht. Krachtens artikel 78 is de Unie bevoegd is de maatregelen vaststellen voor een gemeenschappelijk Europees asielstelsel. Op grond van artikel 79, lid 2, onder c), heeft de Unie de bevoegdheid om maatregelen vast te stellen op het gebied van illegale immigratie en illegaal verblijf. Krachtens artikel 82, lid 1, onder d), en artikel 87, lid 2, onder a), heeft de Unie de bevoegdheid om maatregelen vast te stellen ter bevordering van de politiële en justitiële samenwerking met betrekking tot de verzameling, opslag, verwerking, analyse en uitwisseling van relevante informatie. Krachtens artikel 85, lid 1, en artikel 88, lid 2, is de Unie bevoegd om de taken van respectievelijk Eurojust en Europol te bepalen.

• Subsidiariteit

Vrijheid van verkeer binnen de EU vereist dat de buitengrenzen van de Unie doeltreffend worden beheerd teneinde de veiligheid te waarborgen. De lidstaten zijn dan ook overeengekomen om daar samen voor te zorgen, met name door informatie te delen via gecentraliseerde EU-systemen op het gebied van justitie en binnenlandse zaken. Dit voornemen is bevestigd in de diverse conclusies die met name sinds 2015 zijn vastgesteld door respectievelijk de Europese Raad en de Raad.

De afwezigheid van controles aan de binnengrenzen vereist verstandig beheer van de buitengrenzen van het Schengengebied; elke lidstaat en elk geassocieerd Schengenland moet de buitengrens controleren namens de andere Schengenlanden. Derhalve kan geen enkele lidstaat zelfstandig het hoofd bieden aan irreguliere migratie en grensoverschrijdende criminaliteit. Wanneer onderdanen van derde landen het gebied zonder controles aan de binnengrenzen eenmaal zijn binnengekomen, kunnen zij zich er vrij bewegen. In een gebied zonder binnengrenzen dient tegen irreguliere immigratie, internationale criminaliteit en terrorisme gezamenlijk te worden opgetreden, onder meer door identiteitsfraude op te sporen. Een dergelijke aanpak kan alleen op EU-niveau succesvol zijn.

Op EU-niveau zijn al belangrijke gemeenschappelijke informatiesystemen voorhanden en anders worden zij momenteel ingevoerd. Om de interoperabiliteit van deze

informatiesystemen te versterken, is optreden op EU-niveau geboden. Het voorstel is er in de eerste plaats op gericht de doeltreffendheid en het gebruik van de door eu-LISA beheerde gecentraliseerde systemen te bevorderen. Door de omvang, de effecten en de impact van de voorgestelde maatregelen kunnen de fundamentele doelstellingen alleen doeltreffend en systematisch worden bereikt op EU-niveau.

- **Evenredigheid**

Zoals uitvoerig wordt beschreven in de effectbeoordeling bij dit voorstel voor een verordening, worden de in dit voorstel gemaakte beleidskeuzes als evenredig beschouwd. Zij gaan niet verder dan hetgeen nodig is om de overeengekomen doelstellingen te verwezenlijken.

Het **Europees zoekportaal (ESP)** is een noodzakelijk instrument voor het versterken van het toegestane gebruik van de bestaande en toekomstige EU-informatiesystemen. De impact van het ESP uit het oogpunt van gegevensverwerking is zeer beperkt. Er worden geen gegevens in opgeslagen, afgezien van informatie over de diverse gebruikersprofielen van het ESP en de gegevens en informatiesystemen waartoe de gebruikers toegang hebben. Het gebruik wordt geregistreerd in logbestanden. Krachtens de mandaten zoals die zijn vervat in de rechtsgrondslagen voor de informatiesystemen en de voorgestelde verordening inzake interoperabiliteit is de rol van het ESP als "messagebroker", draaischijf en facilitator evenredig, noodzakelijk en beperkt wat betreft zoekopdrachten en toegangsrechten.

De **gezamenlijke dienst voor biometrische matching (gezamenlijke BMS)** is noodzakelijk voor de werking van het ESP, het gemeenschappelijke identiteitenregister en de detector van meerdere identiteiten. Ook vereenvoudigt deze dienst het gebruik en onderhoud van de bestaande en toekomstige relevante EU-informatiesystemen. De gezamenlijke BMS maakt het mogelijk om op doeltreffende, naadloze en systematische wijze te zoeken in biometrische gegevens uit diverse bronnen. De biometrische gegevens worden opgeslagen en bewaard in de onderliggende systemen. De gezamenlijke BMS genereert templates, maar slaat de eigenlijke afbeeldingen niet op. De gegevens worden dus slechts eenmaal, op één locatie opgeslagen.

Het **gemeenschappelijke identiteitenregister (CIR)** is nodig om een onderdaan van een derde land correct te kunnen identificeren, bv. bij een identiteitscontrole in het Schengengebied. Het CIR ondersteunt ook de werking van de detector van meerdere identiteiten en is derhalve nodig ter verwezenlijking van het tweeledige doel de identiteitscontroles voor bonafide reizigers te vergemakkelijken en identiteitsfraude te bestrijden. Alleen gebruikers die deze informatie nodig hebben voor de uitvoering van hun taken, hebben toegang tot het CIR (en de controle daarvan moet dan ook een nieuwe nevendoelstelling worden van Eurodac, het VIS, het toekomstige EES, het voorgestelde ETIAS en het voorgestelde ECRIS-TCN). De gegevensverwerking wordt strikt beperkt tot wat nodig is om dit doel te bereiken en er zullen passende waarborgen worden vastgesteld om te verzekeren dat de toegangsrechten worden geëerbiedigd en dat in het CIR uitsluitend de minimaal noodzakelijke gegevens worden opgeslagen. Om de gegevensverwerking te minimaliseren en ongerechtvaardigde duplicatie van gegevens te voorkomen, bevat het CIR de vereiste biografische gegevens van elk van de onderliggende systemen (opgeslagen, toegevoegd, gewijzigd en gewist, overeenkomstig hun respectieve rechtsgrondslag), zonder deze te kopiëren. De gegevensbewaringstermijnen zijn volledig in overeenstemming met de gegevensbewaringsvoorschriften van de onderliggende informatiesystemen waaraan de identiteitsgegevens worden ontleend.

De **detector van meerdere identiteiten (MID)** heeft als tweeledig doel identiteitscontroles voor bonafide reizigers te vergemakkelijken en identiteitsfraude te bestrijden. De MID zal de links bevatten tussen natuurlijke personen die in meer dan één centraal informatiesysteem voorkomen. Daarbij gaat het nadrukkelijk alleen om de gegevens die nodig zijn om te controleren of een persoon al dan niet rechtmatig in verschillende systemen onder diverse biografische identiteiten geregistreerd staat dan wel om te verduidelijken dat het bij twee personen met gelijkende biografische gegevens niet om dezelfde persoon hoeft te gaan. De gegevensverwerking door middel van de MID en de gezamenlijke BMS om links aan te brengen tussen afzonderlijke bestanden in afzonderlijke systemen wordt tot een absoluut minimum beperkt. De MID zal waarborgen bevatten tegen mogelijke discriminatie of ongunstige beslissingen jegens personen met meerdere wettelijke identiteiten.

- **Keuze van het instrument**

Het voorgestelde instrument is een verordening van het Europees Parlement en de Raad. De voorgestelde wetgeving heeft rechtstreeks betrekking op de werking van de centrale EU-informatiesystemen voor grenzen en veiligheid, die ofwel op grond van een verordening tot stand zijn gekomen ofwel ten aanzien waarvan is voorgesteld deze tot stand te brengen op grond van een verordening. Ook eu-LISA, dat verantwoordelijk zal zijn voor het ontwerp en de ontwikkeling, en mettertijd ook voor het technisch beheer van de componenten, is opgericht krachtens een verordening. Een verordening is dus het geschikte instrument.

3. RAADPLEGINGEN VAN BELANGHEBBENDEN EN EFFECTBEOORDELINGEN

- **Openbare raadpleging**

Ter voorbereiding van dit voorstel is de Commissie in juli 2017 een openbare raadpleging gestart om de standpunten van geïnteresseerde belanghebbenden over interoperabiliteit te verzamelen. De raadpleging leverde 18 reacties op van uiteenlopende belanghebbenden, waaronder overheden van de lidstaten, particuliere organisaties, organisaties zoals ngo's en denktanks, alsook particuliere burgers[33]. Over het algemeen onderschreven de respondenten de onderliggende beginselen van dit voorstel inzake interoperabiliteit. De overgrote meerderheid van de respondenten was het erover eens dat bij de raadpleging de juiste kwesties aan de orde werden gesteld en dat de doelstellingen van het interoperabiliteitspakket juist zijn. De respondenten waren met name van mening dat de in het raadplegingsdocument geschetste opties:

- het personeel in de praktijk helpen toegang te krijgen tot de informatie die zij nodig hebben;
- zouden voorkomen dat gegevens meermaals worden verzameld, elkaar zouden overlappen of onderling afwijkingen zouden vertonen;
- personen – met inbegrip van personen met meerdere identiteiten – betrouwbaarder wijze zouden identificeren en identiteitsfraude zouden terugdringen.

Een duidelijke meerderheid van de respondenten steunde elk van de voorgestelde opties en achtte deze noodzakelijk voor het bereiken van de doelstellingen van dit initiatief. In hun antwoorden benadrukten deze respondenten de noodzaak van krachtige en duidelijke gegevensbeschermingsmaatregelen, met name in verband met de toegang tot de in de systemen opgeslagen informatie en gegevensbewaring, en wezen zij erop dat er in de

[33] Nadere details zijn te vinden in het samenvattend verslag bij de effectbeoordeling.

systemen actuele, hoogwaardige gegevens dienen te worden opgenomen en dat maatregelen moeten worden getroffen om daarvoor te zorgen.

Met alle bovenstaande punten is bij het opstellen van dit voorstel rekening gehouden.

- **Eurobarometer-enquête**

In juni 2017 is een speciale Eurobarometer-enquête[34] gehouden, waaruit blijkt dat de strategie van de EU om ter bestrijding van criminaliteit en terrorisme informatie op EU-niveau te delen, op grote steun onder de bevolking kan rekenen: bijna alle respondenten (92 %) vinden dat de nationale autoriteiten informatie zouden moeten delen met de autoriteiten van andere lidstaten met het oog op een betere bestrijding van criminaliteit en terrorisme.

Een duidelijke meerderheid (69 %) van de respondenten stelde zich op het standpunt dat de politie en andere nationale wetshandhavingsinstanties informatie op stelselmatige basis zouden moeten uitwisselen met andere EU-landen. In alle lidstaten vindt een meerderheid van de respondenten dat informatie in alle gevallen zou moeten worden gedeeld.

- **Deskundigengroep op hoog niveau inzake informatiesystemen en interoperabiliteit**

Zoals reeds ter sprake is gebracht in de inleiding, vloeit het onderhavige voorstel voort uit de aanbevelingen van de **deskundigengroep op hoog niveau inzake informatiesystemen en interoperabiliteit**[35]. Deze groep is in juni 2016 opgericht om de juridische, technische en operationele problemen aan te pakken in verband met de opties die voor handen zijn om interoperabiliteit tussen centrale EU-systemen voor grenzen en veiligheid tot stand te brengen. De groep werkte vanuit een brede en alomvattende kijk op de architectuur voor gegevensbeheer inzake grensbeheer en rechtshandhaving, en hield tevens rekening met de rol, de bevoegdheden en de systemen van douaneautoriteiten.

De leden van de groep waren deskundigen van de lidstaten en de geassocieerde Schengenlanden en van de EU-agentschappen eu-LISA, Europol, het Europees Ondersteuningsbureau voor asielzaken, het Europees Grens- en kustwachtagentschap en het Bureau van de Europese Unie voor de grondrechten. Ook de coördinator voor terrorismebestrijding van de EU en de Europese Toezichthouder voor gegevensbescherming hadden als gewone leden zitting in de deskundigengroep. Daarnaast traden vertegenwoordigers van het secretariaat van de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken van het Europees Parlement (LIBE) en van het secretariaat-generaal van de Raad op als waarnemer.

Het **eindverslag van deze deskundigengroep op hoog niveau** is in mei 2017 gepubliceerd[36]. In het verslag werd aangedrongen op het verhelpen van de structurele tekortkomingen die waren vastgesteld in de mededeling van april 2016. Het bevat een reeks aanbevelingen om de informatiesystemen van de EU en hun interoperabiliteit te verbeteren. De conclusie luidt dat

---

[34] In het verslag over de standpunten van de Europeanen over veiligheid worden de resultaten geanalyseerd van de speciale Eurobarometer-enquête (464b) over het bewustzijn, de ervaringen en de perceptie van burgers waar het gaat om veiligheid. Deze enquête is van 13 tot en met 26 juni 2017 in 28 lidstaten uitgevoerd door het netwerk van TNS Political & Social. Er werden ongeveer 28 093 EU-burgers uit verschillende sociale en demografische categorieën geïnterviewd.

[35] Besluit van de Commissie van 17 juni 2016 tot oprichting van een deskundigengroep op hoog niveau inzake informatiesystemen en interoperabiliteit (2016/C 257/03).

[36] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

het **noodzakelijk en technisch haalbaar is om als oplossing voor interoperabiliteit te streven naar een Europees zoekportaal, een gezamenlijke dienst voor biometrische matching en een gemeenschappelijk identiteitenregister**, en dat deze in beginsel operationele voordelen kunnen opleveren en kunnen worden vastgesteld met inachtneming van de voorschriften inzake gegevensbescherming. Ook beval de groep aan de aanvullende optie te overwegen van een tweefasenaanpak voor rechtshandhavingsdoeleinden, op basis van een mogelijkheid om treffers te markeren.

Deze ontwerpverordening beantwoordt tevens aan de aanbevelingen van de deskundigengroep op hoog niveau over gegevenskwaliteit, het Universal Message Format (UMF) en de totstandbrenging van een datapakhuis (hier gepresenteerd als het centrale register voor rapportage en statistieken (CRRS)).

De vierde interoperabiliteitscomponent van deze ontwerpverordening (de detector van meerdere identiteiten) is niet aangedragen door de deskundigengroep op hoog niveau, maar is voortgevloeid uit een aanvullende technische analyse en de door de Commissie verrichte evenredigheidsbeoordeling.

- **Technische studies**

Ter ondersteuning van de voorbereiding van het voorstel heeft de Commissie drie studies laten uitvoeren. In opdracht van de Commissie presenteerde Unisys een verslag van een haalbaarheidsstudie voor het Europees zoekportaal. eu-LISA gaf Gartner (en Unisys) opdracht voor een technisch verslag ter ondersteuning van de ontwikkeling van de gezamenlijke dienst voor biometrische matching. PWC bezorgde de Commissie een technisch verslag over een gemeenschappelijk register van identiteitsgegevens.

- **Effectbeoordeling**

Dit voorstel wordt ondersteund door een effectbeoordeling, die is opgenomen in het begeleidende werkdocument van de diensten van de diensten van de Commissie SWD(2017) XXX.

De raad voor regelgevingstoetsing heeft op zijn vergadering van 6 december 2017 de ontwerp-effectbeoordeling bestudeerd en op 8 december haar oordeel gegeven (gunstig, met punten van voorbehoud). Opgemerkt werd dat de effectbeoordeling op bepaalde punten diende te worden aangepast overeenkomstig de door de Raad geformuleerde aanbevelingen. Deze aanbevelingen betroffen in de eerste plaats aanvullende maatregelen in het kader van de voorkeursoptie, om de bestaande gegevenstoegangsrechten van de eindgebruikers in de informatiesystemen te stroomlijnen; ook werd aanbevolen daarmee samenhangende waarborgen voor gegevensbescherming en grondrechten te illustreren. Het tweede belangrijke streven bestond erin de integratie van het Schengeninformatiesysteem onder optie 2 toe te lichten. Daarbij moest ook worden ingegaan op de doeltreffendheid en de kosten, zodat deze optie beter kon worden vergeleken met voorkeursoptie 3. De Commissie werkte haar effectbeoordeling bij om gevolg te geven aan deze belangrijke overwegingen en een aantal andere opmerkingen van de raad.

Bij de effectbeoordeling is geëvalueerd of en zo ja hoe elk van de geformuleerde doelstellingen zou kunnen worden bereikt met behulp van een of meer van de door de deskundigengroep op hoog niveau vastgestelde technische componenten en door middel van daaropvolgende analyse. Waar nodig werd tevens gekeken naar de subopties die nodig zijn

om deze doelstellingen te halen, met inachtneming van het kader voor gegevensbescherming. De conclusie van de effectbeoordeling luidde als volgt:

- ter verwezenlijking van de doelstelling om bevoegde gebruikers te voorzien van snelle, naadloze, systematische en gecontroleerde toegang tot relevante informatiesystemen, dient een Europees zoekportaal (ESP) te worden gecreëerd, op basis van een gezamenlijke dienst voor biometrische matching (gezamenlijke BMS) die alle databanken bestrijkt;
- ter verwezenlijking van de doelstelling om door gemachtigde ambtenaren verrichte identiteitscontroles van onderdanen van derde landen op het grondgebied van een lidstaat te vergemakkelijken, dient op basis van dezelfde gezamenlijke BMS een gemeenschappelijk identiteitenregister (CIR) te worden gecreëerd, dat de minimale reeks identificatiegegevens bevat;
- ter verwezenlijking van de doelstelling om meerdere aan dezelfde reeks biometrische gegevens gelinkte identiteiten op te sporen, teneinde zowel identiteitscontroles voor bonafide reizigers te vergemakkelijken als identiteitsfraude te bestrijden, dient een detector van meerdere identiteiten te worden gebouwd, die links bevat tussen meerdere identiteiten in verschillende systemen;
- ter verwezenlijking van de doelstelling om de toegang van rechtshandhavingsinstanties tot niet voor rechtshandhaving bedoelde informatiesystemen te vergemakkelijken en te stroomlijnen, met het oog op preventie, opsporing, onderzoek of vervolging van zware criminaliteit en terrorisme, dient aan het CIR de mogelijkheid te worden toegevoegd treffers te markeren.

Aangezien aan alle doelstellingen moet worden voldaan, bestaat de **complete oplossing in een combinatie van het ESP, het CIR (met treffermarkering) en de MID, telkens met gebruik van de gezamenlijke BMS**.

De belangrijkste positieve impact zal bestaan in beter grensbeheer en grotere interne veiligheid van de Europese Unie. De nieuwe componenten zullen de toegang van de nationale autoriteiten tot de nodige informatie en identificatie van onderdanen van derde landen stroomlijnen en versnellen. De autoriteiten zullen hierdoor bij grenscontroles, de behandeling van visum- of asielaanvragen en politiewerk dwarsverbanden kunnen leggen met bestaande essentiële, informatie over natuurlijke personen. Hierdoor kan toegang worden verkregen tot informatie die ertoe kan bijdragen dat betrouwbare besluiten worden genomen, of het nu gaat om onderzoek van zware criminaliteit en terrorisme of om besluiten op het gebied van migratie en asiel. Hoewel de voorstellen geen rechtstreekse gevolgen zullen hebben voor burgers van de EU (de voorgestelde maatregelen hebben in de eerste plaats betrekking op onderdanen van derde landen wier gegevens zijn opgenomen in gecentraliseerde informatiesysteem van de EU), zullen zij naar verwachting leiden tot een groter vertrouwen onder de bevolking, doordat het ontwerp en de toepassing van de maatregelen de veiligheid van de EU-burgers bevorderen.

De onmiddellijke financiële en economische effecten van het voorstel beperken zich tot het ontwerp, de ontwikkeling en het beheer van de nieuwe faciliteiten. De kosten zullen ten laste komen van de EU-begroting en van de instanties van de lidstaten die de systemen beheren. De gevolgen voor het toerisme zullen positief zijn, aangezien de voorgestelde maatregelen enerzijds de veiligheid van de Europese Unie zullen verbeteren en anderzijds ook tot snellere grenscontroles zouden moeten leiden. Ook voor luchthavens, zeehavens en vervoerders zullen

de gevolgen naar verwachting positief zijn, met name door het snellere verloop van de grenscontroles.

- **Grondrechten**

Bij de effectbeoordeling is met name gekeken naar de gevolgen van de voorgestelde maatregelen uit het oogpunt van de grondrechten, en met name het recht op gegevensbescherming.

Overeenkomstig het Handvest van de grondrechten van de EU, waaraan de instellingen van de Unie en de lidstaten gehouden zijn wanneer zij het recht van de Unie ten uitvoer brengen (artikel 51, lid 1, van het Handvest), moet een balans worden gevonden tussen enerzijds de kansen die interoperabiliteitsmaatregelen bieden voor de versterking van de veiligheid en de bescherming van de buitengrens en anderzijds de verplichting te waarborgen dat iedere inmenging in de grondrechten die uit de nieuwe interoperabiliteitsomgeving kan voortvloeien, strikt noodzakelijk is om daadwerkelijk te voldoen aan de nagestreefde doelstellingen van algemeen belang, met inachtneming van het evenredigheidsbeginsel (artikel 52, 1, van het Handvest).

De voorgesteld interoperabiliteitsoplossingen bestaan uit componenten die complementair zijn aan de bestaande systemen. Zij zouden dan ook geen verandering moeten brengen in het evenwicht dat de bestaande centrale systemen reeds waarborgen wat betreft hun positieve effect op de grondrechten.

Interoperabiliteit zou niettemin een aanvullend, indirect effect kunnen hebben uit het oogpunt van een aantal grondrechten. Zo heeft de correcte identificatie van een natuurlijke persoon een positief effect op het recht op eerbiediging van het privéleven (artikel 7 van het Handvest), en met name op het recht op identiteit, aangezien het identiteitsverwarring kan helpen voorkomen. Het verrichten van controles op basis van biometrische gegevens kan echter ook worden beschouwd als strijdig met de waardigheid van de betrokkene (artikel 1), met name wanneer deze controles als vernederend worden ervaren. In een enquête[37] van het Bureau van de Europese Unie voor de grondrechten is de respondenten specifiek gevraagd of zij van mening waren dat het laten registreren van hun biometrische gegevens in de context van grenstoezicht vernederend zou kunnen zijn. De meerderheid van de respondenten had niet de indruk dat dit het geval zou zijn.

De voorgestelde interoperabiliteitscomponenten bieden de kans om gerichte preventieve maatregelen vast te stellen ter verbetering van de veiligheid. Zo kunnen zij bijdragen tot de bescherming van het recht op leven (artikel 2 van het Handvest), hetgeen voor de autoriteiten een positieve verplichting inhoudt om preventieve operationele maatregelen te nemen ter bescherming van een natuurlijke persoon wiens leven in gevaar is, als zij weet hebben of gehad zouden moeten hebben van een directe dreiging[38], en om het verbod van slavernij en dwangarbeid (artikel 5) te handhaven. Door identificatie betrouwbaar, toegankelijker en gemakkelijker te maken, kan interoperabiliteit bijdragen tot de opsporing van vermiste kinderen en van kinderen die het slachtoffer van mensenhandel zijn, en snel en gericht optreden mogelijk maken.

---

[37] *FRA survey in the framework of the eu-LISA pilot on smart borders — travellers' views on and experiences of smart borders*, verslag van het Bureau van de Europese Unie voor de grondrechten: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf.

[38] Europees Hof voor de Rechten van de Mens, Osman/Verenigd Koninkrijk, nr. 87/1997/871/1083, 28 oktober 1998, punt 116.

Een betrouwbaar, toegankelijker en eenvoudiger identificatie zou ook kunnen bijdragen tot een doeltreffende handhaving van het asielrecht (artikel 18 van het Handvest) en het verbod van refoulement (artikel 19 van het Handvest). Interoperabiliteit zou namelijk kunnen voorkomen dat asielzoekers op onwettige wijze worden opgepakt en vastgezet en ten onrechte worden uitgezet. Voorts maakt interoperabiliteit het gemakkelijker om identiteitsfraude vast te stellen. Ook zou interoperabiliteit het minder noodzakelijk maken om gegevens en informatie over asielzoekers te delen met derde landen (met name het land van herkomst) teneinde de identiteit van de betrokkene vast te stellen en reisdocumenten te verkrijgen, hetgeen de betrokkene in gevaar zou kunnen brengen.

- **Bescherming van persoonsgegevens**

Interoperabiliteit zal vooral gevolgen hebben voor het recht op de bescherming van persoonsgegevens. Dit recht is vastgelegd in artikel 8 van het Handvest, artikel 16 van het Verdrag betreffende de werking van de Europese Unie en artikel 8 van het Europees Verdrag voor de rechten van de mens. Zoals het Hof van Justitie van de Europese Unie heeft beklemtoond[39], heeft het recht op bescherming van persoonsgegevens geen absolute gelding, maar moet het in relatie tot de functie ervan in de maatschappij worden beschouwd[40]. Er bestaat een nauw verband tussen gegevensbescherming en de eerbiediging van het privéleven en het familie- en gezinsleven, dat door artikel 7 van het Handvest wordt beschermd.

Volgens de algemene verordening gegevensbescherming[41] dient het vrije verkeer van persoonsgegevens in de Unie niet te worden beperkt om redenen die verband houden met gegevensbescherming. Er moet echter wel een aantal beginselen worden geëerbiedigd. Zo kunnen aan de uitoefening van de in het Handvest erkende grondrechten alleen in rechte beperkingen worden gesteld, als wordt voldaan aan de navolgende criteria, die zijn vastgelegd in artikel 52, lid 1, van het Handvest:

- de beperkingen moeten bij wet worden gesteld;
- zij moeten de wezenlijke inhoud van de rechten eerbiedigen;
- zij moeten daadwerkelijk aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen beantwoorden;
- zij moeten noodzakelijk zijn; en
- zij moeten evenredig zijn.

In het huidige voorstel zijn al deze regels inzake gegevensbescherming geïntegreerd, zoals

[39] Arrest van het Hof van Justitie van de EU van 9.11.2010 in gevoegde zaken C-92/09 en C-93/09, Volker und Markus Schecke en Eifert [2010], Jurispr. blz. I-0000/ECLI:EU:C:2010:662.

[40] Artikel 52, lid 1, van het Handvest van de grondrechten bepaalt dat beperkingen op de uitoefening van het recht op gegevensbescherming bij wet moeten worden gesteld en de wezenlijke inhoud van die rechten en vrijheden moeten eerbiedigen, en dat, met inachtneming van het evenredigheidsbeginsel slechts beperkingen kunnen worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

[41] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

uitvoerig wordt uiteengezet in de effectbeoordeling bij dit voorstel voor een verordening. Het voorstel is gebaseerd op de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen. Het omvat alle passende voorschriften, waardoor alleen gegevens worden verwerkt die nodig zijn voor een bepaald doel en toegang alleen wordt verleend op "need to know"-basis. De gegevensbewaringstermijnen (indien van toepassing) zijn passend en beperkt. De toegang is uitsluitend voorbehouden aan de naar behoren gemachtigde personeelsleden van de autoriteiten van de lidstaten en de EU-organen die bevoegd zijn voor de specifieke doelen van elk informatiesysteem, en geldt enkel voor de gegevens die vereist zijn voor de uitvoering van hun taken overeenkomstig deze doelen.

4. GEVOLGEN VOOR DE BEGROTING

De gevolgen voor de begroting zijn opgenomen in het financieel memorandum bij dit voorstel. Het memorandum bestrijkt de resterende periode van het huidige meerjarig financieel kader (tot 2020) en de zeven jaar van de daaropvolgende periode (2021-2027). De voorgestelde begroting voor de jaren 2021 en daarna is opgenomen ter illustratie en loopt niet vooruit op het volgende meerjarig financieel kader.

De uitvoering van dit voorstel vereist begrotingstoewijzingen voor:

(1) De **ontwikkeling** en integratie door eu-LISA van de vier interoperabiliteitscomponenten en het centrale register voor rapportage en statistieken, alsmede het daaropvolgende **onderhoud en beheer**.

(2) De **migratie van gegevens** naar de gezamenlijke dienst voor biometrische matching (gezamenlijke BMS) en het gemeenschappelijke identiteitenregister (CIR). Wat de gezamenlijke BMS betreft, dienen de biometrische templates van de overeenkomstige gegevens uit de drie systemen die momenteel gebruikmaken van biometrische gegevens (SIS, VIS en Eurodac), opnieuw te worden aangemaakt in de gezamenlijke BMS. In het geval van het CIR dienen de persoonsgegevens uit het VIS te migreren naar het CIR en is validering nodig van de mogelijke links die worden ontdekt tussen identiteiten in het SIS, het VIS en Eurodac. Met name dit laatste proces vergt veel middelen.

(3) De modernisering door eu-LISA van de **nationale uniforme interface** (NUI), die reeds is opgenomen in de EES-verordening en een generieke component moet worden voor de uitwisseling van berichten tussen de lidstaten en de centrale systemen.

(4) De **integratie van de nationale systemen van de lidstaten** en de NUI die de berichten doorgeeft die met het CIR/de detector van meerdere identiteiten zijn uitgewisseld via het Europees zoekportaal.

(5) De **opleiding** inzake het gebruik van de interoperabiliteitscomponenten door de eindgebruikers, met name het Agentschap van de Europese Unie voor opleiding op het gebied van rechtshandhaving (Cepol).

De interoperabiliteitscomponenten worden opgebouwd en beheerd als een programma. Terwijl het Europees zoekportaal (ESP) en de detector van meerdere identiteiten geheel nieuwe componenten zijn, evenals het centrale register voor rapportage en statistieken (CRRS), zijn de gezamenlijke BMS en het CIR gezamenlijke componenten die bestaande gegevens die reeds in bestaande of nieuwe systemen opgenomen zijn (of zullen worden), combineren, en dat binnen hun bestaande budgettaire ramingen.

Het **ESP** zal bestaande, bekende interfaces met het SIS, het VIS en Eurodac implementeren en te zijner tijd worden uitgebreid naar nieuwe systemen.

Het ESP zal worden benut door lidstaten en agentschappen door middel van een interface die gebaseerd is op het Universal Message Format (UMF). Voor deze nieuwe interface zullen de lidstaten, eu-LISA, Europol en het Europees Grens- en kustwachtagentschap moeten zorgen voor ontwikkeling, aanpassing, integratie en testen. Het ESP moet gebruikmaken van de concepten van de voor het EES ingevoerde nationale uniforme interface (NUI), waardoor de integratie een minder grote inspanning zal vergen.

Het ESP zal aanvullende kosten voor Europol meebrengen, doordat de Quest-interface beschikbaar moet worden gemaakt voor gebruik met gegevens waarop het basisbeschermingsniveau van toepassing is.

De basis van de **gezamenlijke BMS** zal de facto worden vastgesteld met de oprichting van het nieuwe EES, aangezien dit veruit de meeste nieuwe biometrische gegevens omvat. Het vereiste budget is gereserveerd voor het EES-rechtsinstrument. Het aan de gezamenlijke BMS toevoegen van meer biometrische gegevens uit het VIS, het SIS en Eurodac gaat gepaard met extra kosten, die hoofdzakelijk samenhangen met de migratie van bestaande gegevens. Voor de drie systemen zou in totaal naar schatting 10 miljoen EUR nodig zijn. Het toevoegen van nieuwe biometrische gegevens vanuit het voorgestelde ECRIS-TCN brengt beperkte extra kosten mee, die kunnen worden gedekt door de middelen die voor het voorgestelde ECRIS-TCN-rechtsinstrument zijn gereserveerd, met het oog op de totstandbrenging van een geautomatiseerd ECRIS-TCN-vingerafdrukidentificatiesysteem.

Het **gemeenschappelijke identiteitenregister**, dat tot stand komt wanneer het toekomstige EES wordt opgezet en dat verder zal worden uitgebreid bij de ontwikkeling van het voorgestelde ETIAS. De opslag en de zoekmachines voor deze gegevens zijn opgenomen in het budget dat is gereserveerd voor het toekomstige EES en het voorgestelde ETIAS. De toevoeging van nieuwe biografische gegevens uit Eurodac en het voorgestelde ECRIS-TCN gaat gepaard met weinig extra kosten, in verband waarmee al middelen zijn gereserveerd voor deze rechtsinstrumenten.

Het totale budget dat voor negen jaar (2019-2027) nodig is, beloopt 424,7 miljoen EUR; het dekt de navolgende posten.

(1) Een budget van 225 miljoen EUR voor eu-LISA heeft betrekking op de totale kosten voor de ontwikkeling van een programma dat de vijf interoperabiliteitscomponenten tot stand moet brengen (68,3 miljoen EUR), de onderhoudskosten van het moment dat de componenten gereed zijn tot en met 2027 (56,1 miljoen EUR), een specifiek budget van 25 miljoen EUR voor de migratie van gegevens uit bestaande systemen naar de gezamenlijke BMS en de aanvullende kosten voor de modernisering, het netwerk, opleidingen en vergaderingen inzake de NUI. Een specifiek budget van 18,7 miljoen EUR dekt de kosten van het upgraden en beheren van ECRIS-TCN in hogebeschikbaarheidsmodus vanaf 2022.

(2) Een budget van 136,3 miljoen EUR voor de lidstaten, ter dekking van de kosten van de veranderingen in hun nationale systemen voor het gebruik van de interoperabiliteitscomponenten, de door eu-LISA ontwikkelde NUI en de opleiding van de aanzienlijke groep eindgebruikers.

(3) Een begroting van 48,9 miljoen EUR voor Europol, ter dekking van de kosten van de

upgrade van zijn IT-systemen met het oog op het te verwerken aantal berichten en ter dekking van de kosten van de betere prestaties[42]. De interoperabiliteitscomponenten zullen door het ETIAS worden gebruikt om de gegevens van Europol te raadplegen.

(4) Een budget van 4,8 miljoen EUR voor het Europees Grens- en kustwachtagentschap, ter bekostiging van een team van deskundigen dat gedurende één jaar de links tussen identiteiten zal valideren wanneer de detector van meerdere identiteiten in werking treedt.

(5) Een budget van 2,0 miljoen EUR voor het Agentschap van de Europese Unie voor opleiding op het gebied van rechtshandhaving (Cepol), ter dekking van de voorbereiding en uitvoering van opleiding voor het operationele personeel.

(6) Een voorziening van 7,7 miljoen EUR voor DG HOME, ter dekking van de kosten van een beperkte personeelsuitbreiding en van daarmee samenhangende kosten gedurende de ontwikkelingsfase van de verschillende componenten, aangezien de Commissie gedurende die periode ook aanvullende taken zal moeten uitvoeren en de verantwoordelijkheid op zich neemt voor de met het Universal Message Format belaste commissie.

De verordening inzake het Fonds voor interne veiligheid (ISF) – Grenzen is het financiële instrument waarin het budget voor de uitvoering van het interoperabiliteitsinitiatief is opgenomen. In artikel 5, lid 5, onder b), is daarom voorzien in een bedrag van 791 miljoen EUR voor de ontwikkeling van IT-systemen gebaseerd op bestaande en/of nieuwe IT-systemen ter beheersing van de migratiestromen langs de buitengrenzen, mits de desbetreffende wetgevingshandelingen van de Unie worden vastgesteld, en onder de voorwaarden van artikel 15, lid 5. Van deze 791 miljoen EUR is 480,2 miljoen EUR gereserveerd voor de ontwikkeling van het EES, 210 miljoen EUR voor het ETIAS en 67,9 miljoen EUR voor de herziening van het SIS. De rest (32,9 miljoen EUR) dient te worden herschikt via de ISF-B-mechanismen. Met het onderhavige voorstel is 32,1 miljoen EUR gemoeid voor de looptijd van het huidige meerjarig financieel kader (2019/20); dit bedrag past binnen het resterende budget.

5. AANVULLENDE INFORMATIE

• Uitvoeringsplanning en regelingen betreffende controle, evaluatie en rapportage

Eu-LISA is verantwoordelijk voor het operationele beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht. Als zodanig is het belast met de exploitatie en de technische en operationele verbeteringen van bestaande systemen en met de ontwikkeling van de reeds geplande systemen. Volgens dit voorstel voor een verordening zal eu-LISA het ontwerp van de fysieke architectuur van de interoperabiliteitscomponenten bepalen, de componenten ontwikkelen en implementeren, en deze ten slotte ook hosten. De respectieve componenten zullen geleidelijk worden geïmplementeerd, naargelang de onderliggende systemen worden ontwikkeld.

[42] Met de huidige informatieverwerkingscapaciteit van Europol kunnen de aanzienlijke volumes (gemiddeld 100 000 zoekopdrachten per dag) en de snellere reacties die nodig zullen zijn voor het ETIAS, niet worden verwezenlijkt.

De Commissie zal ervoor zorgen dat er systemen zijn om toezicht te houden op de ontwikkeling en de werking van de vier componenten (Europees zoekportaal, gezamenlijke dienst voor biometrische matching, gemeenschappelijk identiteitenregister, detector van meerdere identiteiten) en het centrale register voor rapportage en statistieken, en deze toetsen aan de belangrijkste beleidsdoelstellingen. Vier jaar na de invoering en operationalisering van de functies van deze componenten, en vervolgens om de vier jaar, dient eu-LISA aan het Europees Parlement, de Raad en de Commissie een verslag voor te leggen over de technische werking van de interoperabiliteitscomponenten. Bovendien dient de Commissie vijf jaar na de invoering en operationalisering van de functies een algemene evaluatie van de componenten te presenteren en daarbij ook stil te staan bij de directe en indirecte gevolgen die de componenten en de praktische implementatie daarvan hebben uit het oogpunt van de grondrechten. Zij dient de behaalde resultaten te toetsen aan de doelstellingen, de onverminderde geldigheid van de uitgangspunten te beoordelen en de implicaties voor toekomstige opties na te gaan. De beoordelingsverslagen dienen aan het Europees Parlement en de Raad te worden voorgelegd.

- **Artikelsgewijze toelichting**

Hoofdstuk I bevat de algemene bepalingen van deze verordening. Het gaat om: de beginselen die aan de verordening ten grondslag liggen, de bij de verordening ingestelde componenten, de doelstellingen van interoperabiliteit, het toepassingsgebied van de verordening, de omschrijving van de in de verordening gebruikte termen en het beginsel van non-discriminatie wat betreft de gegevensverwerking krachtens de verordening.

In hoofdstuk II staan de bepalingen inzake het Europees zoekportaal (ESP). Dit hoofdstuk voorziet in de totstandkoming van het ESP en de technische architectuur daarvan, die door eu-LISA zal worden ontwikkeld. Het doel van het ESP wordt genoemd en er wordt vastgesteld wie het ESP mogen gebruiken en hoe de gebruikers daarbij te werk moeten gaan, gelet op de bestaande toegangsrechten voor elk van de centrale systemen. Bepaald wordt dat eu-LISA gebruikersprofielen aanmaakt voor elke categorie gebruikers. Dit hoofdstuk regelt hoe het ESP de centrale systemen zal doorzoeken en bevat bepalingen inzake de vorm en de inhoud van de antwoorden aan de gebruikers. Verder bepaalt hoofdstuk II dat eu-LISA logs dient bij te houden van alle verwerkingsoperaties en voorziet het in de vangnetprocedure voor het geval dat het ESP geen toegang heeft tot een of meer van de centrale systemen.

Hoofstuk III bevat bepalingen inzake de gezamenlijke dienst voor biometrische matching (gezamenlijke BMS). Dit hoofdstuk regelt de totstandkoming van de gezamenlijke BMS en de technische architectuur daarvan, die door eu-LISA zal worden ontwikkeld. Ook wordt uiteengezet wat het doel is van de gezamenlijke BMS en welke gegevens erin worden opgeslagen. Voorts wordt de relatie tussen de gezamenlijke BMS en de andere componenten uitgelegd. Ten slotte bepaalt hoofdstuk III dat de gezamenlijke BMS gegevens niet blijft bewaren wanneer deze niet meer in het respectieve centrale systeem staan en dat eu-LISA logs bijhoudt van alle verwerkingen.

In hoofdstuk IV staan de bepalingen inzake het gemeenschappelijke identiteitenregister (CIR). Dit hoofdstuk voorziet in de totstandkoming van het CIR en de technische architectuur daarvan, die door eu-LISA zal worden ontwikkeld. Het bepaalt het doel van het CIR en legt uit welke gegevens zullen worden opgeslagen, en hoe. Ook bevat dit hoofdstuk bepalingen die de kwaliteit van de opgeslagen gegevens moeten waarborgen. Voorts wordt in hoofdstuk IV geregeld dat het CIR afzonderlijke bestanden aanmaakt op basis van de in de centrale systemen opgenomen gegevens en dat individuele bestanden worden bijgewerkt als er veranderingen in de individuele centrale systemen worden aangebracht. Ook beschrijft hoofdstuk IV hoe het CIR werkt met betrekking tot de detector van meerdere identiteiten.

Bepaald wordt wie er toegang hebben tot het CIR en hoe die personen toegang tot de gegevens kunnen verkrijgen overeenkomstig de toegangsrechten. Ook bevat het hoofdstuk meer specifieke bepalingen, die van toepassing zijn naargelang het gaat om toegang die identificatie ten doel heeft of – als de eerste fase van de tweefasenaanpak – om toegang tot het EES, het VIS, het ETIAS en Eurodac via het CIR voor rechtshandhavingsdoeleinden. Hoofdstuk IV schrijft ook voor dat eu-LISA logs bijhoudt van de verwerkingen met betrekking tot het CIR.

Hoofdstuk V bevat de bepalingen inzake de detector van meerdere identiteiten (MID). Dit hoofdstuk voorziet in de totstandkoming van de MID en de technische architectuur daarvan, die door eu-LISA zal worden ontwikkeld. Het doel van de MID wordt uitgelegd en het gebruik van de MID overeenkomstig de toegangsrechten voor elk van de centrale systemen wordt geregeld. Hoofdstuk V bepaalt wanneer en hoe de MID overgaat tot het zoeken naar meervoudige identiteiten, hoe de resultaten worden aangeleverd en welk gevolg hieraan wordt gegeven, zo nodig via handmatige controle. Hoofdstuk V bevat een classificatie van de soorten links die kunnen voortvloeien uit de zoekopdracht, naargelang deze gegevens betreffende één identiteit, meerdere identiteiten of een gedeelde identiteit oplevert. Dit hoofdstuk bepaalt dat de MID gelinkte gegevens die in de centrale systemen staan, opslaat, terwijl de gegevens in twee of meer individuele centrale systemen worden bewaard. Hoofdstuk V bepaalt ook dat eu-LISA logs bijhoudt van alle verwerkingsactiviteiten in verband met de MID.

Hoofdstuk VI voorziet in maatregelen ter ondersteuning van de interoperabiliteit. Het voorziet in de mogelijkheid de gegevenskwaliteit te verbeteren, het Universal Message Format vast te stellen als gemeenschappelijke standaard voor informatie-uitwisseling ter ondersteuning van interoperabiliteit, en een centraal register voor rapportage en statistieken in te stellen.

Hoofdstuk VII betreft gegevensbescherming. Het bevat bepalingen die waarborgen dat de krachtens deze verordening verwerkte gegevens op rechtmatige en passende wijze worden verwerkt, overeenkomstig de bepalingen van Verordening nr. 45/2001. Verder wordt uitgelegd wie voor elk van de in deze verordening voorgestelde interoperabiliteitsmaatregelen de gegevensverwerker is en welke maatregelen eu-LISA en de autoriteiten van de lidstaten moeten nemen voor het waarborgen van de beveiliging van de gegevensverwerking, de vertrouwelijkheid van de gegevens, de passende behandeling van veiligheidsincidenten en het passende toezicht op de naleving van de in deze verordening vervatte maatregelen. Het hoofdstuk bevat ook bepalingen over de rechten van de betrokkenen, waaronder het recht te worden geïnformeerd dat gegevens over hen krachtens deze verordening zijn opgeslagen en verwerkt, alsook het recht om toegang te krijgen tot krachtens deze verordening opgeslagen en verwerkte persoonsgegevens. In dit hoofdstuk wordt ook het beginsel vastgesteld dat de krachtens deze verordening verwerkte gegevens niet mogen worden doorgegeven aan of ter beschikking gesteld van derde landen, internationale organisaties of derden, met uitzondering van Interpol (voor een aantal specifieke doeleinden) en van gegevens die van Europol zijn ontvangen via het Europees zoekportaal, waarvoor de regels van Verordening 2016/794 inzake verdere gegevensverwerking gelden. Ten slotte bevat het hoofdstuk de bepalingen inzake toezicht en audit met betrekking tot gegevensbescherming.

Hoofdstuk VIII beschrijft de verantwoordelijkheden van eu-LISA voor en na de inwerkingtreding van de maatregelen in dit voorstel, alsmede de verantwoordelijkheden van de lidstaten, Europol en de centrale ETIAS-eenheid.

Hoofdstuk IX bevat gegevens over: de vereisten inzake rapportage en statistieken in verband met de krachtens deze verordening verwerkte gegevens, de nodige overgangsmaatregelen, regelingen inzake de kosten die uit deze verordening voortvloeien, de vereisten inzake

kennisgevingen, het proces voor de aanvang van de in deze verordening voorgestelde activiteiten, governanceregelingen, onder meer inzake de samenstelling van een comité en een adviesgroep, de taken van eu-LISA op het gebied van opleiding en een praktische handleiding ter ondersteuning van de implementatie en het beheer van de interoperabiliteitscomponenten, procedures voor het toezicht op en de evaluatie van de in deze verordening voorgestelde maatregelen en een bepaling inzake de inwerkingtreding van deze verordening.

2017/0352 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

tot vaststelling van een kader voor interoperabiliteit tussen de EU-informatiesystemen (politiële en justitiële samenwerking, asiel en migratie)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 16, lid 2, artikel 74, artikel 78, lid 2, onder e), artikel 79, lid 2, onder c), artikel 82, lid 1, onder d), artikel 85, lid 1, artikel 87, lid 2, onder a), en artikel 88, lid 2,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Na raadpleging van de Europese Toezichthouder voor gegevensbescherming,

Gezien het advies van het Europees Economisch en Sociaal Comité[43],

Gezien het advies van het Comité van de Regio's[44],

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) In haar mededeling *Krachtigere en slimmere informatiesystemen voor grenzen en veiligheid*[45] van 6 april 2016 heeft de Commissie benadrukt dat de EU-architectuur voor gegevensbeheer voor grensbeheer en veiligheid moest worden verbeterd. De mededeling gaf de aanzet tot een proces dat moet leiden tot interoperabiliteit tussen de EU-informatiesystemen voor veiligheid, grensbeheer en migratiebeheer, om de structurele tekortkomingen in verband met deze systemen te verhelpen, die het werk van de nationale instanties hinderen, en ervoor te zorgen dat grenswachters, douaneautoriteiten, politieambtenaren en gerechtelijke autoriteiten over de nodige informatie beschikken.

(2) In zijn *routekaart voor het verbeteren van informatie-uitwisseling en informatiebeheer op het gebied van justitie en binnenlandse zaken* van 6 juni 2016[46] heeft de Raad verscheidene juridische, technische en operationele problemen in verband met de interoperabiliteit van de EU-informatiesystemen geïdentificeerd en ertoe opgeroepen daar oplossingen voor te vinden.

(3) In zijn resolutie van 6 juli 2016 over de strategische prioriteiten met betrekking tot het werkprogramma van de Commissie voor 2017[47] heeft het Europees Parlement

[43] PB C […] van […], blz. […].

[44]

[45] COM(2016) 205 van 6.4.2016.

[46] Routekaart van 6 juni 2016 voor het verbeteren van informatie-uitwisseling en informatiebeheer op het gebied van justitie en binnenlandse zaken, onder meer door middel van interoperabiliteitsoplossingen – 9368/1/16 REV 1.

[47] Resolutie van het Europees Parlement van 6 juli 2016 over de strategische prioriteiten met betrekking tot het werkprogramma van de Commissie voor 2017 (2016/2773(RSP).

aangedrongen op voorstellen om de bestaande EU-informatiesystemen te verbeteren en verder te ontwikkelen, informatieleemten aan te pakken en de interoperabiliteit tussen voornoemde systemen te bevorderen, en op voorstellen voor verplichte gegevensuitwisseling op EU-niveau, samen met de nodige waarborgen voor gegevensbescherming.

(4) De Europese Raad van 15 december 2016[48] heeft gevraagd om te blijven werken aan de interoperabiliteit van informatiesystemen en databanken.

(5) In zijn eindverslag van 11 mei 2017[49] heeft de deskundigengroep inzake informatiesystemen en interoperabiliteit geconcludeerd dat het noodzakelijk en technisch haalbaar is om praktische oplossingen voor interoperabiliteit na te streven, en dat deze in beginsel zowel operationele voordelen kunnen opleveren als met inachtneming van de voorschriften inzake gegevensbescherming kunnen worden vastgesteld.

(6) In haar mededeling van 16 mei 2017 (*Zevende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie*[50]) heeft de Commissie, overeenkomstig haar mededeling van 6 april 2016 en conform de bevindingen en aanbevelingen van de deskundigengroep op hoog niveau, een nieuwe aanpak beschreven voor het beheer van gegevens voor grenzen, veiligheid en migratie, waarbij alle gecentraliseerde EU-informatiesystemen voor veiligheid, grensbeheer en migratiebeheer interoperabel zijn, met volledige inachtneming van de grondrechten.

(7) In zijn conclusies van 9 juni 2017[51] over de verdere stappen voor het verbeteren van de informatie-uitwisseling en het waarborgen van de interoperabiliteit van de EU-informatiesystemen, heeft de Raad de Commissie verzocht om de door de deskundigengroep op hoog niveau voorgestelde oplossingen inzake operabiliteit na te streven.

(8) De Europese Raad van 23 juni 2017[52] heeft de noodzaak onderstreept van een verbetering van de interoperabiliteit tussen databanken en de Commissie verzocht zo spoedig mogelijk ontwerpwetgeving op te stellen en daarin de voorstellen uit te werken van de deskundigengroep op hoog niveau inzake informatiesystemen en interoperabiliteit.

(9) Teneinde het beheer van de buitengrenzen te verbeteren, bij te dragen aan het voorkomen en bestrijden van irreguliere migratie en aan een hoog niveau van veiligheid in de ruimte van vrijheid, veiligheid en recht van de Unie, met inbegrip van handhaving van de openbare orde en veiligheid en de vrijwaring van de veiligheid op het grondgebied van de lidstaten, dient er interoperabiliteit tot stand te worden gebracht tussen een aantal EU-informatiesystemen, namelijk het inreis-uitreissysteem (EES), het Visuminformatiesysteem (VIS), [het Europees systeem voor reisinformatie en -autorisatie (ETIAS)], Eurodac, het Schengeninformatiesysteem (SIS) en [het Europees Strafregister Informatiesysteem voor onderdanen van derde landen (ECRIS-TCN)], opdat deze EU-informatiesystemen en de erin opgenomen gegevens elkaar aanvullen. Hiertoe dienen de volgende interoperabiliteitscomponenten tot stand te worden gebracht: een Europees zoekportaal (ESP), een gezamenlijke dienst voor

---

48 http://www.consilium.europa.eu/nl/press/press-releases/2016/12/15/euco-conclusions-final/.
49 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.
50 COM(2017) 261 final van 16.5.2017.
51 http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf.
52 Conclusies van de Europese Raad, 22-23 juni 2017.

biometrische matching (gezamenlijke BMS), een gemeenschappelijk identiteitenregister (CIR) en een detector van meerdere identiteiten (MID).

(10) De interoperabiliteit tussen de informatiesystemen van de EU moet deze systemen in staat stellen elkaar aan te vullen teneinde de correcte identificatie van personen te vergemakkelijken, bijdragen tot de bestrijding van identiteitsfraude, vereisten inzake de gegevenskwaliteit van de respectieve Europese informatiesystemen verbeteren en harmoniseren, de technische en operationele implementatie van de bestaande en de toekomstige informatiesystemen van de EU door de lidstaten vergemakkelijken, de waarborgen inzake gegevensbeveiliging en -bescherming die van toepassing zijn op de informatiesystemen van de EU versterken en vereenvoudigen, en de toegang van rechtshandhavingsinstanties tot het EES, het VIS, het [ETIAS] en Eurodac stroomlijnen en de doelen van het EES, het VIS, het [ETIAS], Eurodac, het SIS en het [ECRIS-TCN] ondersteunen.

(11) De interoperabiliteitscomponenten dienen betrekking te hebben op het EES, het VIS, het ETIAS, Eurodac, het SIS en het [ECRIS-TCN]. Voornoemde componenten dienen ook van toepassing te zijn op de gegevens van Europol, in de zin dat zij het mogelijk moeten maken de gegevens van Europol gelijktijdig met de EU-informatiesystemen te doorzoeken.

(12) De interoperabiliteitscomponenten moeten betrekking hebben op personen van wie persoonsgegevens in de EU-informatiesystemen en door Europol worden verwerkt, namelijk onderdanen van derde landen van wie persoonsgegevens in de EU-informatiesystemen en door Europol worden verwerkt alsook EU-burgers van wie persoonsgegevens in het SIS en door Europol worden verwerkt.

(13) Het Europees zoekportaal (ESP) dient te worden opgericht om het langs technische weg gemakkelijker te maken voor de autoriteiten van de lidstaten en de EU-organen om snel, ononderbroken, efficiënt, systematisch en gecontroleerd toegang te krijgen tot de EU-informatiesystemen, de gegevens van Europol en de databanken van Interpol die zij nodig hebben om hun taken te verrichten, zulks overeenkomstig hun toegangsrechten en ter ondersteuning van de doelstellingen van het EES, het VIS, het [ETIAS], Eurodac, het SIS, het [ECRIS-TCN] en de gegevens van Europol. Door het mogelijk te maken gelijktijdig en parallel te zoeken in alle relevante EU-informatiesystemen, alsook in de gegevens van Europol en de databanken van Interpol, moet het ESP dienstdoen als één loket of "messagebroker" voor het naadloos doorzoeken van verscheidene centrale systemen en opvragen van de nodige informatie, met volledige inachtneming van de voorschriften inzake toegangscontrole en gegevensbescherming van de onderliggende systemen.

(14) ESP-eindgebruikers met recht op toegang tot de gegevens van Europol op grond van Verordening (EU) 2016/794 van het Europees Parlement en de Raad[53] moeten gelijktijdig kunnen zoeken in de gegevens van Europol en in de EU-informatiesystemen waartoe zij toegang hebben. Elke verdere verwerking van gegevens na een dergelijke zoekopdracht moet plaatsvinden in overeenstemming met Verordening (EU) 2016/794, ook wat door de gegevensverstrekker opgelegde beperkingen op de toegang of het gebruik van de gegevens betreft.

[53] Verordening (EU) 2016/794 van het Europees Parlement en de Raad van 11 mei 2016 betreffende het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol) en tot vervanging en intrekking van de Besluiten 2009/371/JBZ, 2009/934/JBZ, 2009/935/JBZ, 2009/936/JBZ en 2009/968/JBZ van de Raad (PB L 135 van 24.5.2016, blz. 53).

(15) Het Europees zoekportaal (ESP) dient zodanig te worden ontwikkeld en geconfigureerd dat het niet mogelijk is bij de zoekopdracht gegevensvelden te gebruiken die geen verband houden met personen of reisdocumenten of die niet in een informatiesysteem van de EU, in de gegevens van Europol of in de databank van Interpol zijn opgenomen.

(16) Om ervoor te zorgen dat alle EU-informatiesystemen snel en systematisch worden gebruikt, dient het Europees zoekportaal (ESP) te worden gebruikt voor het doorzoeken van het gemeenschappelijke identiteitenregister, het EES, het VIS, [het ETIAS], Eurodac en [het ECRIS-TCN] . De nationale verbinding met de verschillende EU-informatiesystemen dient echter te blijven bestaan, bij wijze van technisch vangnet. Het ESP dient ook door organen van de Unie te worden gebruikt om het centrale SIS overeenkomstig hun toegangsrechten te doorzoeken voor het verrichten van hun taken. Het ESP dient een aanvullend middel te zijn voor het doorzoeken van het centrale SIS, de gegevens van Europol en de systemen van Interpol, ter aanvulling van de interfaces die daarvoor al beschikbaar zijn.

(17) Biometrische gegevens zoals vingerafdrukken en gezichtsopnamen zijn uniek en derhalve voor de identificatie van een persoon veel betrouwbaarder dan alfanumerieke gegevens. De gezamenlijke dienst voor biometrische matching (gezamenlijke BMS) dient als technisch instrument het werk van de relevante EU-informatiesystemen en andere interoperabiliteitscomponenten te versterken en vereenvoudigen. De gezamenlijke BMS heeft in de eerste plaats ten doel de identificatie te vergemakkelijken van een natuurlijke persoon die wellicht geregistreerd is in verschillende databanken, door biometrische gegevens tussen verschillende systemen te matchen en door te werken met één enkele technologische component in plaats van vijf afzonderlijke componenten in elk van de onderliggende systemen. De gezamenlijke BMS dient de veiligheid te bevorderen alsmede voordelen uit financieel, operationeel en onderhoudsoogpunt op te leveren, door uit te gaan van één enkele technologische component in plaats van meerdere, per onderliggend systeem verschillende componenten. Alle geautomatiseerde vingerafdrukidentificatiesystemen, waaronder de momenteel voor Eurodac, het VIS en het SIS gebruikte toepassingen, maken gebruik van biometrische templates met gegevens die zijn verkregen door specifieke kenmerken te extraheren uit concrete biometrische informatie. De gezamenlijke BMS dient al deze biometrische templates te bundelen en op één locatie op te slaan, zodat systeemoverschrijdende vergelijkingen op basis van biometrische gegevens gemakkelijker worden en schaalvoordelen bij de ontwikkeling en het onderhoud van de centrale EU-systemen kunnen worden behaald.

(18) Biometrische gegevens zijn gevoelige persoonsgegevens. Deze verordening dient de grondslag en de waarborgen vast te stellen voor de verwerking van dergelijke gegevens met het oog op de unieke identificatie van de betrokkenen.

(19) De systemen die zijn ingesteld bij Verordening (EU) 2017/2226 van het Europees Parlement en de Raad[54], Verordening (EG) nr. 767/2008 van het Europees Parlement

[54] Verordening (EU) 2017/2226 van het Europees Parlement en de Raad van 30 november 2017 tot instelling van een inreis-uitreissysteem (EES) voor de registratie van inreis- en uitreisgegevens en van gegevens over weigering van toegang ten aanzien van onderdanen van derde landen die de buitengrenzen overschrijden en tot vaststelling van de voorwaarden voor toegang tot het EES voor rechtshandhavingsdoeleinden en tot wijziging van de overeenkomst ter uitvoering van het te Schengen gesloten akkoord en Verordeningen (EG) nr. 767/2008 en (EU) nr. 1077/2011 (EES-verordening) (PB L 327 van 9.12.2017, blz. 20).

en de Raad[55] en [de ETIAS-verordening] voor het beheer van de grenzen van de Unie, het systeem dat is ingesteld bij [de Eurodac-verordening] voor de identificatie van personen die om internationale bescherming verzoeken en de bestrijding van irreguliere migratie, en het systeem dat is ingesteld bij [de ECRIS-TCN-verordening] kunnen alleen doeltreffend zijn als de onderdanen wier persoonsgegevens daarin worden opgeslagen, accuraat zijn geïdentificeerd.

(20) Het gemeenschappelijke identiteitenregister (CIR) dient derhalve de correcte identificatie van personen die zijn geregistreerd in het EES, het VIS, [het ETIAS], Eurodac en [het ECRIS-TCN], te bevorderen en vereenvoudigen.

(21) Persoonsgegevens die in deze EU-informatiesystemen zijn opgeslagen, kunnen betrekking hebben op dezelfde personen, van wie echter verschillende of onvolledige identiteitsgegevens kunnen zijn geregistreerd. De lidstaten beschikken over efficiënte manieren om hun burgers of de geregistreerde permanent ingezetenen op hun grondgebied te identificeren, maar dat geldt niet voor onderdanen van derde landen. De interoperabiliteit tussen de EU-informatiesystemen dient bij te dragen tot de correcte identificatie van onderdanen van derde landen. In het gemeenschappelijke identiteitenregister (CIR) dienen de in de systemen opgenomen persoonsgegevens betreffende onderdanen van derde landen te worden opgeslagen die nodig zijn om de betrokkenen zo accuraat mogelijk te identificeren; het gaat dus onder meer om hun identiteitsgegevens, gegevens van reisdocumenten en biometrische gegevens en het doet er niet toe in welk systeem de gegevens oorspronkelijk werden verzameld. Alleen de persoonsgegevens die strikt noodzakelijk zijn voor een accurate identiteitscontrole dienen in het CIR te worden opgeslagen. De in het CIR opgeslagen persoonsgegevens dienen niet langer te worden bewaard dan strikt noodzakelijk is voor de doeleinden van de onderliggende systemen en dienen automatisch te worden gewist wanneer de gegevens worden verwijderd uit de onderliggende systemen, met inachtneming van de logische scheiding van die systemen.

(22) De nieuwe verwerkingsverrichting die erin bestaat dat die gegevens worden opgeslagen in het gemeenschappelijke identiteitenregister (CIR), in plaats van in elk van de afzonderlijke systemen, is noodzakelijk om de accuratesse te bevorderen van de identificatie die mogelijk wordt gemaakt door het geautomatiseerde vergelijken en matchen van die gegevens. Het feit dat de identiteit en de biometrische gegevens van onderdanen van derde landen in het CIR worden opgeslagen, mag op geen enkele wijze de gegevensverwerking voor de doeleinden van de verordeningen inzake het EES, het VIS, het ETIAS, Eurodac of het ECRIS-TCN verhinderen, aangezien het CIR een nieuwe gezamenlijke component van dergelijke onderliggende systemen dient te zijn.

(23) In dat verband dient voor eenieder die is geregistreerd in het EES, het VIS, het ETIAS, Eurodac of het ECRIS-TCN een afzonderlijk bestand te worden aangelegd in het gemeenschappelijke identiteitenregister, zowel ter verwezenlijking van het doel onderdanen van derde landen in het Schengengebied correct te identificeren als ter ondersteuning van de detector van meerdere identiteiten; het tweeledige doel hiervan is de identiteitscontrole van bonafide reizigers te vergemakkelijken en identiteitsfraude te bestrijden. Dit afzonderlijke bestand dient op één plaats te worden bewaard en

[55] Verordening (EG) nr. 767/2008 van het Europees Parlement en de Raad van 9 juli 2008 betreffende het Visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van gegevens op het gebied van visa voor kort verblijf (VIS-verordening) (PB L 218 van 13.8.2008, blz. 60).

gemachtigde eindgebruikers toegang te bieden tot alle mogelijke identiteiten die aan een persoon zijn gelinkt.

(24) Het gemeenschappelijke identiteitenregister (CIR) dient aldus de werking van de detector van meerdere identiteiten te ondersteunen en de rechtshandhavingsinstanties op eenvoudiger en gestroomlijnde wijze toegang te bieden tot de EU-informatiesystemen die niet uitsluitend zijn ingesteld voor preventie, opsporing, onderzoek of vervolging van ernstige criminaliteit.

(25) Het gemeenschappelijke identiteitenregister (CIR) dient te voorzien in een gedeelde datacontainer voor biometrische en identiteitsgegevens van onderdanen van derde landen die geregistreerd zijn in het EES, het VIS, [het ETIAS], Eurodac en het [ECRIS-TCN], en deze datacontainer moet voor deze systemen fungeren als de gezamenlijke component voor het opslaan en doorzoeken van dergelijke gegevens.

(26) Alle records in het gemeenschappelijke identiteitenregister (CIR) dienen logisch te worden gescheiden door elke record automatisch te voorzien van een label waaruit blijkt van welk onderliggend systeem het deel uitmaakt. Bij de toegangscontrole van het CIR dienen deze te worden gebruikt om te bepalen of een record al dan niet toegankelijk is.

(27) Om de correcte identificatie van een persoon te waarborgen, dient het de autoriteiten van de lidstaten die bevoegd zijn voor het voorkomen en bestrijden van irreguliere migratie en de bevoegde autoriteiten in de zin van artikel 3, lid 7, van Richtlijn 2016/680 te worden toegestaan om het gemeenschappelijke identiteitenregister (CIR) te doorzoeken aan de hand van de tijdens een identiteitscontrole vastgestelde biometrische gegevens van de betrokkene.

(28) Als de biometrische gegevens van de persoon niet kunnen worden gebruikt of wanneer het zoeken aan de hand van die gegevens geen resultaat oplevert, dient te worden gezocht aan de hand van de identiteitsgegevens van de betrokkene in combinatie met gegevens van reisdocumenten. Als de zoekopdracht uitwijst dat er gegevens over de betrokkene zijn opgeslagen in het gemeenschappelijke identiteitenregister (CIR), dienen de autoriteiten van de lidstaten daartoe toegang te hebben om de in het CIR opgeslagen gegevens van de betrokkene te raadplegen, zonder dat op enige wijze wordt duidelijk gemaakt van welk informatiesysteem van de EU die gegevens deel uitmaken.

(29) De lidstaten dienen nationale wetgevingsmaatregelen vast te stellen tot aanwijzing van de instanties die bevoegd zijn voor het uitvoeren van identiteitscontroles met behulp van het gemeenschappelijke identiteitenregister (CIR) en tot vaststelling van de procedures, voorwaarden en criteria van deze controles overeenkomstig het evenredigheidsbeginsel. De nationale wetgevingsmaatregelen dienen met name te voorzien in de bevoegdheid om biometrische gegevens te verzamelen wanneer iemand door een vertegenwoordiger van voornoemde instanties aan een identiteitscontrole wordt onderworpen.

(30) Deze verordening dient het tevens mogelijk te maken om de aangewezen rechtshandhavingsinstanties van de lidstaten alsmede Europol gestroomlijnde toegang te bieden tot andere gegevens dan identiteitsgegevens in het EES, het VIS, [het ETIAS] of Eurodac. De systemen bevatten naast identiteitsgegevens ook andere gegevens die in een specifiek geval noodzakelijk kunnen zijn om terroristische misdrijven of andere ernstige strafbare feiten te voorkomen, op te sporen, te onderzoeken en te vervolgen.

(31) De volledige toegang tot de nodige gegevens in de informatiesystemen van de EU (andere dan de relevante identiteitsgegevens uit het gemeenschappelijk identiteitenregister (CIR) die zijn verkregen door gebruik te maken van tijdens een identiteitscontrole vastgestelde biometrische gegevens) dient, wanneer die toegang noodzakelijk is met het oog op het voorkomen, opsporen en onderzoeken van terroristische misdrijven of andere ernstige strafbare feiten, onderworpen te blijven aan de bepalingen in de respectieve rechtsinstrumenten. De aangewezen rechtshandhavingsinstanties en Europol weten vooraf niet welke EU-informatiesystemen gegevens bevatten van de personen over wie zij informatie nodig hebben. Dit leidt tot vertragingen en inefficiëntie bij de uitvoering van hun taken. De door de aangewezen instantie gemachtigde eindgebruiker dient derhalve te kunnen zien in welke van de EU-informatiesystemen de gegevens betreffende de ingevoerde zoekopdracht worden geregistreerd. Het betrokken systeem moet dus worden gemarkeerd nadat automatisch is geverifieerd dat het systeem een treffer bevat (treffermarkering).

(32) De logbestanden van de zoekopdrachten van het gemeenschappelijke identiteitenregister dienen het doel van de zoekopdracht te vermelden. Als een zoekopdracht is verricht door raadpleging via de tweefasenaanpak, dienen de logbestanden een verwijzing te bevatten naar het nationale dossier van het onderzoek of de zaak en te vermelden dat een dergelijke zoekopdracht is gestart met het oog op het voorkomen, opsporen en onderzoeken van terroristische misdrijven of andere ernstige strafbare feiten.

(33) Wil een zoekopdracht in het gemeenschappelijke identiteitenregister (CIR) door de aangewezen autoriteiten en Europol leiden tot een antwoord met treffermarkering waaruit blijkt dat de gegevens zijn geregistreerd in het EES, het VIS, [het ETIAS] of Eurodac, dan is automatische verwerking van persoonsgegevens vereist. Een treffermarkering dient geen persoonsgegevens te onthullen, maar hoogstens te vermelden dat bepaalde persoonsgegevens van de betrokkene in een van de systemen zijn opgeslagen. De gemachtigde eindgebruiker mag niet louter op grond van een treffermarkering een beslissing nemen die ongunstig is voor de betrokkene. De toegang van een eindgebruiker tot een treffermarkering houdt een zeer beperkte inmenging in het recht op bescherming van de persoonsgegevens van de betrokkene in en is nodig om de aangewezen autoriteit en Europol in staat te stellen hun verzoek om toegang tot persoonsgegevens rechtstreeks te richten tot het systeem dat de gegevens volgens de markering bevat, hetgeen doeltreffender is.

(34) De tweefasenaanpak inzake gegevensraadpleging is met name van belang voor zaken waarin de verdachte, de dader of het mogelijke slachtoffer van een terroristisch misdrijf of ander ernstig strafbaar feit onbekend is. In dergelijke gevallen dient het gemeenschappelijke identiteitenregister (CIR) met een enkele zoekopdracht het informatiesysteem te kunnen identificeren waarin de betrokkene is opgenomen. Door het gebruik van deze nieuwe aanpak inzake de toegang voor rechtshandhavingsdoeleinden in dergelijke gevallen verplicht te stellen, hoeft voordat toegang wordt geboden tot de in het EES, het VIS, [het ETIAS] en Eurodac opgeslagen persoonsgegevens, niet eerst een zoekopdracht te worden verricht in de nationale databanken en een zoekopdracht te worden gestart in het geautomatiseerde vingerafdrukidentificatiesysteem van andere lidstaten krachtens Besluit 2008/615/JHA. Het beginsel dat eerst in nationale databanken moet worden gezocht, beperkt de mogelijkheden van de autoriteiten van de lidstaten om systemen te raadplegen voor rechtmatige rechtshandhavingsdoeleinden, waardoor kansen om

benodigde informatie boven water te krijgen, wellicht onbenut blijven. De vereisten eerst een zoekopdracht te verrichten in de nationale databanken en vervolgens een zoekopdracht te starten in het geautomatiseerde vingerafdrukidentificatiesysteem van andere lidstaten krachtens Besluit 2008/615/JBZ dienen van toepassing te blijven tot de tweefasenaanpak van toegang voor wetshandhavingsdoeleinden via het CIR als alternatieve waarborg volledig operationeel is geworden.

(35) Om de werking van het gemeenschappelijke identiteitenregister te ondersteunen en de doelstellingen van het EES, het VIS, [het ETIAS], Eurodac, het SIS en [het ECRIS-TCN] te bevorderen, dient een detector van meerdere identiteiten (MID) te worden opgezet. Al deze informatiesystemen van de EU kunnen alleen aan hun respectieve doelstellingen beantwoorden, als de personen wier persoonsgegevens erin worden opgeslagen, nauwkeurig worden geïdentificeerd.

(36) De doelstellingen van de informatiesystemen van de EU kunnen vooralsnog niet worden bereikt, doordat de autoriteiten die deze systemen gebruiken, niet in staat zijn om een voldoende betrouwbare verificatie te verrichten van de identiteit van onderdanen van derde landen van wie gegevens in verschillende systemen worden opgeslagen. Dat zij hiertoe niet in staat zijn, komt doordat de reeks identiteitsgegevens die is opgeslagen in een bepaald systeem frauduleus, onjuist of onvolledig kan zijn en het op dit moment niet mogelijk is dergelijke frauduleuze, onjuiste of onvolledige identiteitsgegevens op te sporen door middel van vergelijking met gegevens die zijn opgeslagen in een ander systeem. Om deze situatie te verhelpen, is op het niveau van de Unie een technisch instrument nodig waarmee onderdanen van derde landen voor deze doeleinden accuraat kunnen worden geïdentificeerd.

(37) De detector van meerdere identiteiten (MID) dient links tussen gegevens in de verschillende EU-informatiesystemen aan te brengen en op te slaan, zodat meerdere identiteiten kunnen worden opgespoord, met als tweeledig doel zowel identiteitscontroles voor bonafide reizigers te vergemakkelijken als identiteitsfraude te bestrijden. De MID dient enkel de links te bevatten tussen natuurlijke personen die in meer dan één EU-informatiesysteem voorkomen en daarbij gaat het nadrukkelijk alleen om de gegevens die nodig zijn om te controleren of een persoon al dan niet rechtmatig in verschillende systemen onder diverse biografische identiteiten geregistreerd staat dan wel om te verduidelijken dat het bij twee personen met vergelijkbare biografische gegevens niet om dezelfde persoon hoeft te gaan. De gegevensverwerking via het Europees zoekportaal (ESP) en de gezamenlijke dienst voor biometrische matching (BMS) voor het aanbrengen van links tussen afzonderlijke bestanden in afzonderlijke systemen dient tot het absolute minimum te worden beperkt en gaat dan ook niet verder dan de opsporing van meerdere identiteiten op het moment dat nieuwe gegevens worden toegevoegd aan een van de informatiesystemen die zijn opgenomen in het gemeenschappelijke identiteitsregister en in het SIS. De MID dient waarborgen te bevatten tegen mogelijke discriminatie of ongunstige beslissingen jegens personen met meerdere rechtmatige identiteiten.

(38) Deze verordening voorziet in nieuwe gegevensverwerkingsverrichtingen voor het correct identificeren van de betrokkenen. Dit vormt een inmenging in hun grondrechten die worden beschermd door de artikelen 7 en 8 van het Handvest van de grondrechten. Aangezien de EU-informatiesystemen alleen doeltreffend kunnen worden geïmplementeerd als de betrokkenen correct worden geïdentificeerd, is een dergelijke inmenging gerechtvaardigd op grond van dezelfde doelstellingen als die waarvoor elk van deze systemen tot stand is gebracht, namelijk het doeltreffende beheer van de grenzen van de Unie, de interne veiligheid van de Unie, de

doeltreffende tenuitvoerlegging van het asiel- en visumbeleid van de Unie en de bestrijding van irreguliere migratie.

(39) Het Europees zoekportaal (ESP) en de gezamenlijke dienst voor biometrische matching (gezamenlijke BMS) dienen in het gemeenschappelijke identiteitenregister (CIR) en het SIS opgeslagen gegevens over personen te vergelijken wanneer een nationale autoriteit of een EU-orgaan nieuwe records aanmaakt. Deze vergelijking moet automatisch worden verricht. Het CIR en het SIS dienen het gezamenlijke BMS te gebruiken om mogelijke links op te sporen op basis van biometrische gegevens. Het CIR en het SIS dienen gebruik te maken van het ESP om mogelijke links op basis van alfanumerieke gegevens op te sporen. Het CIR en het SIS dienen identieke of vergelijkbare gegevens over een onderdaan van een derde land in meerdere systemen te kunnen identificeren. In voorkomend geval dient een link te worden aangebracht waaruit blijkt dat het om dezelfde persoon gaat. Het CIR en het SIS dienen zodanig te worden geconfigureerd dat kleine transliteratie- of spelfouten zodanig worden opgemerkt dat de betrokken onderdaan van een derde land geen onnodige hinder ondervindt.

(40) De nationale autoriteit of het EU-orgaan dat de gegevens in het betrokken EU-informatiesysteem heeft geregistreerd, dient deze links te bevestigen of veranderen. Deze autoriteit dient toegang te hebben tot de gegevens die zijn opgeslagen in het gemeenschappelijke identiteitenregister (CIR) of het SIS en in de detector van meerdere identiteiten (MID) met het oog op manuele identiteitsverificatie.

(41) De autoriteiten van de lidstaten en de EU-organen die toegang hebben tot ten minste één EU-informatiesysteem dat is opgenomen in het gemeenschappelijke identiteitenregister, of tot het SIS, dienen slechts toegang tot zogeheten rode links te krijgen, wanneer de gelinkte gegevens dezelfde biometrische gegevens maar andere identiteitsgegevens bevatten en er volgens de autoriteit die verantwoordelijk is voor de verificatie van verschillende identiteiten onrechtmatig naar dezelfde persoon wordt verwezen, of wanneer de gelinkte gegevens vergelijkbare identiteitsgegevens bevatten en er volgens de autoriteit die verantwoordelijk is voor de verificatie van meerdere identiteiten, onrechtmatig naar dezelfde persoon wordt verwezen. Wanneer de gelinkte gegevens niet vergelijkbaar zijn, dient een gele link te worden aangebracht en een manuele verificatie plaats te vinden teneinde de kleur van de link te bevestigen dan wel te veranderen.

(42) De manuele verificatie van meerdere identiteiten dient te worden gewaarborgd door de autoriteit die verantwoordelijk is voor het genereren of bijwerken van de gegevens die leiden tot een treffer naar aanleiding waarvan een link is aangebracht met reeds in een ander EU-informatiesysteem opgeslagen gegevens. De instantie die verantwoordelijk is voor de verificatie van meerdere identiteiten dient te beoordelen of er sprake is van meerdere rechtmatige of onrechtmatige identiteiten. Een dergelijke beoordeling dient, indien mogelijk, te worden uitgevoerd in aanwezigheid van de onderdaan van het derde land en, zo nodig, door om nadere toelichting of informatie te vragen. Een dergelijke beoordeling dient onverwijld te worden uitgevoerd, overeenkomstig de wettelijke voorschriften betreffende de juistheid van informatie op grond van het Unierecht en het nationaal recht.

(43) Voor de links die zijn verkregen in verband met het Schengeninformatiesysteem (SIS) voor signaleringen van personen die worden gezocht met het oog op aanhouding ten behoeve van overlevering of uitlevering, van vermiste of kwetsbare personen, van personen die worden gezocht met het oog op een gerechtelijke procedure, personen die

aan een onopvallende of gerichte controle moeten worden onderworpen, dan wel onbekende gezochte personen, dient de autoriteit die verantwoordelijk is voor de verificatie van meerdere identiteiten het Sirene-bureau te zijn van de lidstaat die de signalering heeft gecreëerd. Deze categorieën SIS-signaleringen zijn namelijk gevoelig en dienen niet per se te worden gedeeld met de autoriteiten die de gegevens in een van de andere EU-informatiesystemen creëren of bijwerken. Het aanbrengen van een link met SIS-gegevens dient de maatregelen die moeten worden genomen overeenkomstig de [SIS-verordeningen] onverlet te laten.

(44) eu-LISA dient geautomatiseerde mechanismen voor de controle van gegevenskwaliteit en gemeenschappelijke indicatoren voor gegevenskwaliteit vast te stellen. eu-LISA dient een centrale controlecapaciteit voor gegevenskwaliteit te ontwikkelen en regelmatig verslag uit te brengen over de gegevenskwaliteit, teneinde de controle te verbeteren van de wijze waarop de lidstaten de EU-informatiesystemen implementeren en toepassen. De gemeenschappelijke kwaliteitsindicatoren dienen de minimumkwaliteitsnormen voor gegevensopslag in de EU-informatiesystemen en de interoperabiliteitscomponenten te omvatten. Met behulp van dergelijke gegevenskwaliteitsnormen dienen de EU-informatiesystemen en interoperabiliteitscomponenten kennelijk onjuiste of inconsistente gegevensinvoer automatisch te kunnen herkennen, zodat de lidstaat die de gegevens heeft ingevoerd deze kan verifiëren en zo nodig corrigerende maatregelen kan nemen.

(45) De Commissie dient de kwaliteitsverslagen van eu-LISA te evalueren en zo nodig aanbevelingen te doen aan de lidstaten. De lidstaten dienen te worden belast met het opstellen van een actieplan met een beschrijving van de maatregelen om tekortkomingen in de kwaliteit van de gegevens te verhelpen en dienen regelmatig verslag uit te brengen over de geboekte voortgang.

(46) Het Universal Message Format (UMF) dient als norm te gelden voor de gestructureerde, grensoverschrijdende informatie-uitwisseling tussen informatiesystemen, autoriteiten en/of organisaties op het gebied van justitie en binnenlandse zaken. In de UMF-norm dienen een gemeenschappelijk vocabularium en logische structuren voor informatie-uitwisseling te worden vastgesteld met als doel de interoperabiliteit te bevorderen door het mogelijk te maken de inhoud van de uitwisseling op een consistente en semantisch gelijkwaardige manier te creëren en te lezen.

(47) Er dient een centraal register voor rapportage en statistieken (CRRS) te worden ingesteld om systeemoverschrijdende statistische gegevens en analytische verslagen te genereren voor doeleinden op het gebied van beleid, operationaliteit en gegevenskwaliteit. eu-LISA dient op zijn technische locaties te zorgen voor het opstellen, implementeren en hosten van het CRRS, met daarin anonieme statistische gegevens van voornoemde systemen, het gemeenschappelijke identiteitenregister, de detector van meerdere identiteiten en de gezamenlijke dienst voor biometrische matching. Het mag niet mogelijk zijn om aan de hand van de in het CRRS opgenomen gegevens personen te identificeren. eu-LISA dient de gegevens te anonimiseren en de geanonimiseerde gegevens te registreren in het CRRS. Het anonimiseren van de gegevens dient automatisch te gebeuren en aan het personeel van eu-LISA mag geen directe toegang worden verleend tot persoonsgegevens die zijn opgeslagen in de informatiesystemen van de EU of de interoperabiliteitscomponenten.

(48) Verordening (EU) 2016/679 dient van toepassing te zijn op de verwerking van persoonsgegevens door de nationale autoriteiten uit hoofde van deze verordening,

tenzij de verwerking wordt verricht door de aangewezen autoriteiten of centrale toegangspunten van de lidstaten met het oog op het voorkomen, onderzoeken of opsporen van terroristische misdrijven of andere ernstige strafbare feiten; in die gevallen dient Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad namelijk van toepassing te zijn.

(49) De specifieke voorschriften inzake gegevensbescherming van [de Eurodac-verordening], [de SIS-verordening op het gebied van rechtshandhaving], [de SIS-verordening op het gebied van de terugkeer van illegaal verblijvende onderdanen van derde landen] en [de ECRIS-TCN-verordening] dienen van toepassing te zijn op de verwerking van persoonsgegevens in die respectieve systemen.

(50) Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad[56] dient van toepassing te zijn op de verwerking van persoonsgegevens door eu-LISA en andere instellingen en organen van de Unie wanneer deze hun taken in het kader van deze verordening uitvoeren, onverminderd Verordening (EU) 2016/794, die dient te gelden voor de verwerking van persoonsgegevens door Europol.

(51) De krachtens [Verordening (EU) 2016/679] ingestelde nationale toezichthoudende autoriteiten dienen toe te zien op de rechtmatigheid van de verwerking van persoonsgegevens door de lidstaten, terwijl de bij Verordening (EG) nr. 45/2001 ingestelde Europese Toezichthouder voor gegevensbescherming toezicht dient uit te oefenen op de werkzaamheden van de instellingen en organen van de Unie in verband met de verwerking van persoonsgegevens. De Europese Toezichthouder voor gegevensbescherming en de toezichthoudende autoriteiten dienen samen te werken bij het toezicht op de verwerking van persoonsgegevens door interoperabiliteitscomponenten.

(52) "(...) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 28, lid 2, van Verordening (EG) nr. 45/2001 en heeft op … een advies uitgebracht."

(53) Wat de vertrouwelijkheid betreft, dienen ambtenaren en andere personeelsleden die werkzaamheden in verband met het SIS verrichten, zich te houden aan de relevante bepalingen van het Statuut van de ambtenaren en de regeling welke van toepassing is op de andere personeelsleden van de Europese Unie.

(54) Zowel de lidstaten als eu-LISA dienen beveiligingsplannen bij te houden om de uitvoering van hun verplichtingen op het gebied van beveiliging te vereenvoudigen, en met elkaar samen te werken om beveiligingsvraagstukken vanuit een gemeenschappelijke invalshoek te benaderen. eu-LISA dient er ook voor te zorgen dat steeds gebruik wordt gemaakt van de meest recente technologische ontwikkelingen teneinde de gegevensintegriteit te waarborgen in verband met de ontwikkeling, het ontwerp en het beheer van de interoperabiliteitscomponenten.

(55) Ter ondersteuning van de rapportage en statistieken is het noodzakelijk toegang te verlenen aan gemachtigde personeelsleden van de in deze verordening bedoelde bevoegde autoriteiten, instellingen en organen, zodat zij bepaalde gegevens kunnen raadplegen die verband houden met bepaalde interoperabiliteitscomponenten, zonder dat individuele identificatie mogelijk wordt gemaakt.

[56] Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (PB L 8 van 12.1.2001, blz. 1).

(56) Om de bevoegde autoriteiten en de EU-organen in staat te stellen zich aan te passen aan de nieuwe vereisten inzake het gebruik van het Europees zoekportaal (ESP), dient er te worden voorzien in een overgangsperiode. Evenzo dienen met het oog op de samenhangende en optimale werking van de detector van meerdere identiteiten (MID) overgangsmaatregelen te worden vastgesteld voor de ingebruikneming ervan.

(57) De kosten in verband met het ontwikkelen van de interoperabiliteitscomponenten worden in het huidige meerjarig financieel kader lager geraamd dan het saldo van de begroting die in Verordening (EU) nr. 515/2014 van het Europees Parlement en de Raad is uitgetrokken voor slimme grenzen[57]. Overeenkomstig artikel 5, lid 5, onder b), van Verordening (EU) nr. 515/2014 dient het bedrag dat thans voor de ontwikkeling van IT-systemen ter beheersing van de migratiestromen over de buitengrenzen is toegewezen, op grond van deze verordening te worden herbestemd.

(58) Ter aanvulling van bepaalde gedetailleerde technische aspecten van deze verordening dient de bevoegdheid om overeenkomstig artikel 290 van het Verdrag betreffende de werking van de Europese Unie handelingen vast te stellen, aan de Commissie worden gedelegeerd met betrekking tot de profielen voor de gebruikers van het Europees zoekportaal (ESP) en de inhoud en het format van de ESP-antwoorden. Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden, onder meer op deskundigenniveau, passende raadplegingen verricht overeenkomstig de beginselen die zijn vastgelegd in het Interinstitutioneel Akkoord over beter wetgeven van 13 april 2016[58]. Met name om te zorgen voor gelijke deelname aan de voorbereiding van gedelegeerde handelingen, dienen het Europees Parlement en de Raad alle documenten op hetzelfde tijdstip te ontvangen als de deskundigen van de lidstaten, en dienen hun deskundigen systematisch toegang te hebben tot de vergaderingen van de deskundigengroepen van de Commissie die zich bezighouden met de voorbereiding van de gedelegeerde handelingen.

(59) Om ervoor te zorgen dat de omstandigheden waarin deze verordening ten uitvoer wordt gelegd, overal dezelfde zijn, dienen aan de Commissie uitvoeringsbevoegdheden te worden toegekend om gedetailleerde regels vast te stellen inzake: de mechanismen, procedures en indicatoren voor de geautomatiseerde controle van gegevenskwaliteit; de ontwikkeling van de UMF-norm; procedures voor het vaststellen van gevallen waarin identiteiten een gelijkenis vertonen; de werking van het centraal register voor rapportage en statistieken; en de procedure voor samenwerking bij veiligheidsincidenten. Deze bevoegdheden dienen te worden uitgeoefend overeenkomstig Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad[59].

(60) Verordening 2016/794 is van toepassing op de verwerking van gegevens voor de doeleinden van deze verordening door Europol.

(61) Deze verordening laat de toepassing van Richtlijn 2004/38/EG onverlet.

---

[57] Verordening (EU) nr. 515/2014 van het Europees Parlement en de Raad van 16 april 2014 tot vaststelling, als onderdeel van het Fonds voor interne veiligheid, van het instrument voor financiële steun voor de buitengrenzen en visa en tot intrekking van Beschikking nr. 574/2007/EG (PB L 150 van 20.5.2014, blz. 143).

[58] http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=uriserv%3AOJ.L_.2016.123.01.0001.01.ENG.

[59] Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren (PB L 55 van 28.2.2011, blz. 13).

(62) Overeenkomstig artikel 3 van de overeenkomst tussen de Europese Gemeenschap en het Koninkrijk Denemarken betreffende de criteria en instrumenten om te bepalen welke staat verantwoordelijk is voor de behandeling van een asielverzoek dat wordt ingediend in Denemarken of een andere lidstaat van de Europese Unie, en betreffende „Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van de Overeenkomst van Dublin[60], dient Denemarken de Commissie ervan in kennis te stellen of het de inhoud van deze verordening zal toepassen, voor zover zij betrekking heeft op Eurodac [en het geautomatiseerde systeem voor registratie en monitoring, en het toewijzingsmechanisme voor verzoeken om internationale bescherming, als bedoeld in artikel 44 van Verordening (EU) XX/XX tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend (herschikking)].

(63) Voor zover de bepalingen van deze verordening betrekking hebben op het SIS, zoals geregeld bij Besluit 2007/533/JBZ, neemt het Verenigd Koninkrijk aan deze verordening deel overeenkomstig artikel 5, lid 1, van het Protocol (nr. 19) betreffende het Schengenacquis dat is opgenomen in het kader van de Europese Unie, dat aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie is gehecht ("protocol betreffende het Schengenacquis"), en overeenkomstig artikel 8, lid 2, van Besluit 2000/365/EG van de Raad van 29 mei 2000 betreffende het verzoek van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland deel te mogen nemen aan enkele van de bepalingen van het Schengenacquis[61]. Voor zover deze verordening betrekking heeft op Eurodac [en het geautomatiseerde systeem voor registratie en monitoring, en het toewijzingsmechanisme voor verzoeken om internationale bescherming, als bedoeld in artikel 44 van Verordening (EU) XX/XX tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend (herschikking)], kan het Verenigd Koninkrijk voorts de voorzitter van de Raad in kennis stellen van zijn wens om deel te nemen aan de vaststelling en toepassing ervan, overeenkomstig artikel 3 van het Protocol (nr. 21) betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, dat aan het VEU en het VWEU is gehecht ("protocol betreffende de positie van het Verenigd Koninkrijk en Ierland"). Voor zover de bepalingen van deze verordening betrekking hebben op [het ECRIS-TCN], neemt het Verenigd Koninkrijk overeenkomstig de artikelen 1 en 2 en artikel 4 bis, lid 1, van het Protocol (nr. 21) betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, dat aan het VEU en het VWEU is gehecht, niet deel aan de vaststelling van deze verordening, die derhalve niet bindend is voor, noch van toepassing is in deze lidstaat. Overeenkomstig artikel 3 en artikel 4 bis, lid 1, van Protocol nr. 21 kan het Verenigd Koninkrijk te kennen geven dat het aan de vaststelling van deze verordening wenst deel te nemen.

(64) Voor zover de bepalingen van deze verordening betrekking hebben op het SIS, zoals geregeld bij Besluit 2007/533/JBZ, neemt Ierland aan deze verordening deel overeenkomstig artikel 5, lid 1, van het Protocol (nr. 19) betreffende het

60

61

Schengenacquis dat is opgenomen in het kader van de Europese Unie, dat aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie is gehecht ("protocol betreffende het Schengenacquis"), en overeenkomstig artikel 6, lid 2, van Besluit 2002/192/EG van de Raad van 28 februari 2002 betreffende het verzoek van Ierland deel te mogen nemen aan bepalingen van het Schengenacquis[62]. Voor zover deze verordening betrekking heeft op Eurodac [en het geautomatiseerde systeem voor registratie en monitoring, en het toewijzingsmechanisme voor verzoeken om internationale bescherming, als bedoeld in artikel 44 van Verordening (EU) XX/XX tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend (herschikking)] kan Ierland voorts de voorzitter van de Raad in kennis stellen van zijn wens om deel te nemen aan de vaststelling en toepassing ervan, overeenkomstig artikel 3 van het Protocol (nr. 21) betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, dat aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie is gehecht ("protocol betreffende de positie van het Verenigd Koninkrijk en Ierland"). Voor zover de bepalingen van deze verordening betrekking hebben op [het ECRIS-TCN], neemt Ierland overeenkomstig de artikelen 1 en 2 en artikel 4 bis, lid 1, van het Protocol (nr. 21) betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, dat aan het VEU en het VWEU is gehecht, niet deel aan de vaststelling van deze verordening, die derhalve niet bindend is voor, noch van toepassing is in deze lidstaat. Overeenkomstig artikel 3 en artikel 4 bis, lid 1, van Protocol nr. 21 kan Ierland te kennen geven dat het aan de vaststelling van deze verordening wenst deel te nemen.

(65) Met betrekking tot IJsland en Noorwegen, en met betrekking tot Eurodac [en het geautomatiseerde systeem voor registratie en monitoring, en het toewijzingsmechanisme voor verzoeken om internationale bescherming, als bedoeld in artikel 44 van Verordening (EU) XX/XX tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend (herschikking)], is deze verordening een nieuwe maatregel in de zin van de Overeenkomst tussen de Europese Gemeenschap, de Republiek IJsland en het Koninkrijk Noorwegen betreffende de criteria en de mechanismen voor de vaststelling van de staat die verantwoordelijk is voor de behandeling van een asielverzoek dat in een lidstaat, in IJsland of in Noorwegen wordt ingediend.

(66) Met betrekking tot Zwitserland, en met betrekking tot Eurodac [en het geautomatiseerde systeem voor registratie en monitoring, en het toewijzingsmechanisme voor verzoeken om internationale bescherming, als bedoeld in artikel 44 van Verordening (EU) XX/XX tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend (herschikking)], is deze verordening een nieuwe maatregel in de zin van de Overeenkomst tussen de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de criteria en mechanismen voor de

62

vaststelling van de staat die verantwoordelijk is voor de behandeling van een asielverzoek dat in een lidstaat of in Zwitserland wordt ingediend.

(67) Met betrekking tot Liechtenstein, en met betrekking tot Eurodac [en het geautomatiseerde systeem voor registratie en monitoring, en het toewijzingsmechanisme voor verzoeken om internationale bescherming, als bedoeld in artikel 44 van Verordening (EU) XX/XX tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend (herschikking)], is deze verordening een nieuwe maatregel in de zin van het Protocol tussen de Europese Gemeenschap, de Zwitserse Bondsstaat en het Vorstendom Liechtenstein betreffende de toetreding van het Vorstendom Liechtenstein tot de Overeenkomst tussen de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de criteria en mechanismen voor de vaststelling van de staat die verantwoordelijk is voor de behandeling van een asielverzoek dat in een lidstaat of in Zwitserland wordt ingediend.

(68) Deze verordening eerbiedigt de grondrechten en de beginselen die met name zijn vastgelegd in het Handvest van de grondrechten van de Europese Unie, en dient te worden toegepast overeenkomstig die rechten en beginselen,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I
Algemene bepalingen

Artikel 1
Onderwerp

1. Bij deze verordening, in combinatie met [Verordening (EU) 2018/xx inzake interoperabiliteit op het gebied van grenzen en visa], wordt een kader vastgesteld dat ervoor moet zorgen dat het inreis-uitreissysteem (EES), het Visuminformatiesysteem (VIS), [het Europees systeem voor reisinformatie en -autorisatie (ETIAS)], Eurodac, het Schengeninformatiesysteem (SIS) en [het Europees Strafregister Informatiesysteem voor onderdanen van derde landen (ECRIS-TCN)] interoperabel zijn en dat deze systemen en de daarin opgenomen gegevens elkaar aanvullen.

2. Het kader bestaat onder meer uit de volgende interoperabiliteitscomponenten:

   (a) een Europees zoekportaal (*European search portal* – ESP);

   (b) een gezamenlijke dienst voor biometrische matching (*biometric matching service* – gezamenlijke BMS);

   (c) een gemeenschappelijk identiteitenregister (*common identity repository* – CIR);

   (d) een detector van meerdere identiteiten (*multiple-identity detector* – MID).

3. De verordening bevat ook bepalingen inzake de vereisten op het gebied van gegevenskwaliteit, inzake een Universal Message Format (UMF) en inzake een centraal register voor rapportage en statistieken (CRRS), alsook een omschrijving van de verantwoordelijkheden van de lidstaten en van het Europees Agentschap voor

het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (eu-LISA) met betrekking tot het ontwerp en de werking van de interoperabiliteitscomponenten.

4. De verordening behelst tevens een aanpassing van de procedures en voorwaarden waaraan de rechtshandhavingsinstanties van de lidstaten en het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol) zich moeten houden om toegang tot het inreis-uitreissysteem (EES), het Visuminformatiesysteem (VIS), [het Europees systeem voor reisinformatie en -autorisatie (ETIAS)] en Eurodac te krijgen met het oog op het voorkomen, opsporen en onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten die onder hun bevoegdheid vallen.

Artikel 2
Doelstellingen van de interoperabiliteit

1. Door de interoperabiliteit te waarborgen, dient deze verordening de volgende doelstellingen:

   (a) verbeteren van het beheer van de buitengrenzen;

   (b) bijdragen tot het voorkomen en bestrijden van irreguliere migratie;

   (c) bijdragen aan een hoog niveau van veiligheid in de ruimte van vrijheid, veiligheid en recht van de Unie, met inbegrip van handhaving van de openbare orde en veiligheid en vrijwaring van de veiligheid op het grondgebied van de lidstaten;

   (d) verbeteren van de uitvoering van het gemeenschappelijk visumbeleid; en

   (e) verlenen van bijstand bij de behandeling van verzoeken om internationale bescherming.

2. De met het waarborgen van de interoperabiliteit nagestreefde doelstellingen worden bereikt door:

   (a) een correcte identificatie van personen te verzekeren;

   (b) bij te dragen tot de bestrijding van identiteitsfraude;

   (c) te zorgen voor betere en geharmoniseerde vereisten inzake gegevenskwaliteit voor de respectieve EU-informatiesystemen;

   (d) de technische en operationele implementatie van bestaande en toekomstige EU-informatiesystemen door de lidstaten te vergemakkelijken;

   (e) de voorwaarden inzake gegevensbeveiliging en -bescherming voor de respectieve EU-informatiesystemen strenger, eenvoudiger en uniformer te maken;

   (f) de voorwaarden voor de toegang van rechtshandhavingsinstanties tot het EES, het VIS, [het ETIAS] en Eurodac te stroomlijnen;

   (g) de doelstellingen van het EES, het VIS, [het ETIAS], Eurodac, het SIS en [het ECRIS-TCN] te ondersteunen.

Artikel 3
Toepassingsgebied

1. Deze verordening is van toepassing op Eurodac, het Schengeninformatiesysteem (SIS) en [het Europees Strafregister Informatiesysteem voor onderdanen van derde landen (ECRIS-TCN)].

2. De verordening is ook van toepassing op de gegevens van Europol, voor zover zij het mogelijk maakt dat de in lid 1 bedoelde informatiesystemen deze gegevens gelijktijdig doorzoeken in overeenstemming met het Unierecht.

3. De verordening is van toepassing op personen ten aanzien van wie persoonsgegevens mogen worden verwerkt in de in lid 1 bedoelde EU-informatiesystemen en in de in lid 2 bedoelde gegevens van Europol.

Artikel 4
Definities

Voor de toepassing van deze verordening wordt verstaan onder:

(1) "buitengrenzen": de buitengrenzen in de zin van artikel 2, punt 2, van Verordening (EU) 2016/399;

(2) "grenscontroles": grenscontroles in de zin van artikel 2, punt 11, van Verordening (EU) 2016/399;

(3) "grensautoriteit": de grenswachter die overeenkomstig het nationaal recht is aangewezen voor het verrichten van grenscontroles;

(4) "toezichthoudende autoriteiten": de krachtens artikel 51, lid 1, van Verordening (EU) 2016/679 ingestelde toezichthoudende autoriteit en de krachtens artikel 41, lid 1, van Richtlijn (EU) 2016/680 ingestelde toezichthoudende autoriteit;

(5) "verificatie": het proces waarbij reeksen gegevens worden vergeleken om vast te stellen of een beweerde identiteit correct is (één-op-éénvergelijking);

(6) "identificatie": het proces waarbij de identiteit van een persoon wordt vastgesteld door middel van een zoekopdracht in een databank en vergelijking met verscheidene reeksen gegevens (één-op-veelvergelijking);

(7) "onderdaan van een derde land": een persoon die geen burger van de Unie is in de zin van artikel 20, lid 1, van het Verdrag, of een staatloze persoon, of een persoon van wie de nationaliteit niet bekend is;

(8) "alfanumerieke gegevens": gegevens die worden weergegeven door letters, cijfers, speciale tekens, spaties en leestekens;

(9) "identiteitsgegevens": de gegevens als bedoeld in artikel 27, lid 3, onder a) tot en met h);

(10) "vingerafdrukgegevens": de gegevens betreffende de vingerafdrukken van een persoon;

(11) "gezichtsopname": een digitale afbeelding van het gezicht;

(12) "biometrische gegevens": vingerafdrukgegevens en/of gezichtsopname;

(13) "biometrische template": een mathematische weergave die wordt verkregen door uit biometrische gegevens uitsluitend de kenmerken te extraheren die nodig zijn voor identificatie- en verificatiedoeleinden;

(14) "reisdocument": een paspoort of een ander gelijkwaardig document dat de houder ervan het recht geeft de buitengrenzen te overschrijden en waarin een visum kan worden aangebracht;

(15) "reisdocumentgegevens": het type en nummer van het reisdocument, de naam en drielettercode van het land dat het reisdocument heeft afgegeven, en de datum waarop de geldigheidstermijn van het reisdocument verstrijkt;

(16) "reisautorisatie": een reisautorisatie in de zin van artikel 3 van [de ETIAS-verordening];

(17) "visum voor kort verblijf": een visum in de zin van artikel 2, punt 2, onder a), van Verordening (EG) nr. 810/2009;

(18) "EU-informatiesystemen": de door eu-LISA beheerde grootschalige IT-systemen;

(19) "gegevens van Europol": persoonsgegevens die door Europol zijn verstrekt voor het in artikel 18, lid 2, onder a), van Verordening (EU) 2016/794 bedoelde doel;

(20) "databanken van Interpol": de Interpol-databank voor gestolen en verloren reisdocumenten (SLTD) en de Interpol-databank voor reisdocumenten met signaleringen (TDAWN);

(21) "match": een verband dat aan het licht wordt gebracht door het vergelijken van tweemaal of vaker voorkomende persoonsgegevens die in een informatiesysteem of databank zijn of worden geregistreerd;

(22) "treffer": de bevestiging van een of meer matches;

(23) "politieautoriteit": "bevoegde autoriteit" in de zin van artikel 3, punt 7, van Richtlijn (EU) 2016/680;

(24) "aangewezen autoriteiten": de aangewezen autoriteiten van de lidstaten als bedoeld in artikel 29, lid 1, van Verordening (EU) 2017/2226, artikel 3, lid 1, van Besluit 2008/633/JBZ van de Raad, [artikel 43 van de ETIAS-verordening] en [artikel 6 van de Eurodac-verordening];

(25) "terroristisch misdrijf": een strafbaar feit naar nationaal recht dat overeenkomt met of gelijkwaardig is aan een van de strafbare feiten bedoeld in Richtlijn (EU) 2017/541;

(26) "ernstig strafbaar feit": een strafbaar feit dat overeenkomt met of gelijkwaardig is aan een van de strafbare feiten bedoeld in artikel 2, lid 2, van Kaderbesluit 2002/584/JBZ, indien het volgens het nationaal recht strafbaar is gesteld met een vrijheidsstraf of een tot vrijheidsbeneming strekkende maatregel met een maximumduur van ten minste drie jaar;

(27) "EES": het inreis-uitreissysteem als bedoeld in Verordening (EU) 2017/2226;

(28) "VIS": het Visuminformatiesysteem als bedoeld in Verordening (EG) nr. 767/2008;

(29) [ETIAS": het Europees Systeem voor reisinformatie en -autorisatie als bedoeld in de ETIAS-verordening];

(30) "Eurodac": Eurodac als bedoeld in de [Eurodac-verordening];

(31) "SIS": het Schengeninformatiesysteem als bedoeld [in de SIS-verordening op het gebied van grenscontroles, de SIS-verordening op het gebied van rechtshandhaving en de SIS-verordening op het gebied van de terugkeer van illegaal verblijvende onderdanen van derde landen];

(32) ["ECRIS-TCN": het Europees Strafregister Informatiesysteem met informatie inzake veroordelingen van onderdanen van derde landen en staatlozen als bedoeld in de verordening inzake het ECRIS-TCN];

(33) "ESP": het Europees zoekportaal als bedoeld in artikel 6;

(34) "gezamenlijke BMS": de gezamenlijke dienst voor biometrische matching als bedoeld in artikel 15;

(35) "CIR": het gemeenschappelijke identiteitenregister als bedoeld in artikel 17;

(36) "MID": de detector van meerdere identiteiten als bedoeld in artikel 25;

(37) "CRRS": het centrale register voor rapportage en statistieken als bedoeld in artikel 39.

Artikel 5
Non-discriminatie

De verwerking van persoonsgegevens voor de toepassing van deze verordening mag niet leiden tot discriminatie van personen op grond van, onder meer, geslacht, ras of etnische afstamming, godsdienst of overtuiging, handicap, leeftijd of seksuele geaardheid. Bij de verwerking worden de menselijke waardigheid en integriteit ten volle gerespecteerd. Bijzondere aandacht wordt geschonken aan kinderen, ouderen en personen met een handicap.

HOOFDSTUK II
Het Europees zoekportaal

Artikel 6
Het Europees zoekportaal

1. Er wordt een Europees zoekportaal (ESP) ingesteld om ervoor te zorgen dat de autoriteiten van de lidstaten en de EU-organen snel, ononderbroken, efficiënt, systematisch en gecontroleerd toegang hebben tot de EU-informatiesystemen, de gegevens van Europol en de databanken van Interpol die zij nodig hebben om hun taken te verrichten overeenkomstig hun toegangsrechten en ter ondersteuning van de doelstellingen van het EES, het VIS, [het ETIAS], Eurodac, het SIS, [het ECRIS-TCN] en de gegevens van Europol.

2. Het ESP bestaat uit:

   (a) een centrale infrastructuur, inclusief een zoekportaal voor het gelijktijdig doorzoeken van het EES, het VIS, [het ETIAS], Eurodac, het SIS, [het ECRIS-TCN], alsmede van de gegevens van Europol en de databanken van Interpol;

   (b) een beveiligd communicatiekanaal tussen het ESP, de lidstaten en de EU-organen die overeenkomstig het Unierecht gebruik mogen maken van het ESP;

   (c) een beveiligde communicatie-infrastructuur tussen het ESP en het EES, het VIS, [het ETIAS], Eurodac, het centrale SIS, [het ECRIS-TCN)], de gegevens

van Europol en de databanken van Interpol, alsmede tussen het ESP en de centrale infrastructuur van het CIR en de MID.

3. eu-LISA zorgt voor de ontwikkeling en het technische beheer van het ESP.

Artikel 7
Gebruik van het Europees zoekportaal

1. Het gebruik van het ESP is voorbehouden aan de autoriteiten van de lidstaten en de EU-organen die overeenkomstig het Unierecht of het desbetreffend nationaal recht toegang hebben tot het EES, [het ETIAS], het VIS, het SIS, Eurodac, [het ECRIS-TCN], het CIR en de MID, alsmede tot de gegevens van Europol en de databanken van Interpol.

2. De in lid 1 bedoelde autoriteiten gebruiken het ESP om overeenkomstig hun toegangsrechten uit hoofde van het Unierecht of het nationaal recht gegevens over personen of hun reisdocumenten te doorzoeken in de centrale systemen van Eurodac en [het ECRIS-TCN]. Zij maken eveneens gebruik van het ESP om overeenkomstig hun toegangsrechten uit hoofde van deze verordening het CIR te doorzoeken voor de doeleinden bedoeld in de artikelen 20, 21 en 22.

3. De in lid 1 bedoelde autoriteiten van de lidstaat kunnen het ESP gebruiken om gegevens over personen of hun reisdocumenten te doorzoeken in het centrale SIS bedoeld in [de SIS-verordening op het gebied van grenscontroles en de SIS-verordening op het gebied van rechtshandhaving]. De toegang tot het centrale SIS via het ESP wordt tot stand gebracht door het nationale systeem (N.SIS) van elke lidstaat overeenkomstig [artikel 4, lid 2, van de SIS-verordening op het gebied van grenscontroles en de SIS-verordening op het gebied van rechtshandhaving].

4. EU-organen gebruiken het ESP voor het doorzoeken van gegevens over personen of hun reisdocumenten in het centrale SIS.

5. De in lid 1 bedoelde autoriteiten kunnen het ESP gebruiken om overeenkomstig hun toegangsrechten uit hoofde van het Unierecht of het nationaal recht gegevens over personen of hun reisdocumenten te doorzoeken in de gegevens van Europol.

Artikel 8
Profielen voor de gebruikers van het Europees zoekportaal

1. Om het gebruik van het ESP mogelijk te maken, maakt eu-LISA in overeenstemming met de in lid 2 bedoelde technische details en toegangsrechten en overeenkomstig het Unierecht en het nationaal recht een profiel aan voor elke categorie van ESP-gebruikers, met daarin:

   (a) de voor de zoekopdrachten te gebruiken datavelden;

   (b) de verplicht en facultatief te raadplegen EU-informatiesystemen, gegevens van Europol en databanken van Interpol die de gebruiker van een antwoord zullen voorzien; en

   (c) de in elk antwoord te verstrekken gegevens.

2. De Commissie stelt overeenkomstig artikel 63 gedelegeerde handelingen vast waarin de in lid 1 bedoelde profielen van de in artikel 7, lid 1, bedoelde ESP-gebruikers

technisch worden gespecificeerd in overeenstemming met de respectieve toegangsrechten.

Artikel 9
Zoekopdrachten

1. De ESP-gebruikers starten een zoekopdracht door gegevens in het ESP in te voeren overeenkomstig hun gebruikersprofiel en toegangsrechten. Zodra een zoekopdracht is gegeven, gebruikt het ESP de door de ESP-gebruiker ingevoerde gegevens om het EES, [het ETIAS], het VIS, het SIS, Eurodac, [het ECRIS-TCN] en het CIR, alsmede de gegevens van Europol en de databanken van Interpol gelijktijdig te doorzoeken.

2. De datavelden die worden gebruikt om via het ESP een zoekopdracht te starten, komen overeen met de datavelden betreffende personen of reisdocumenten die mogen worden gebruikt om de verschillende EU-informatiesystemen, de gegevens van Europol en de databanken van Interpol overeenkomstig de respectieve rechtsinstrumenten te doorzoeken.

3. eu-LISA implementeert voor het ESP een interface control document (ICD) op basis van de in artikel 38 bedoelde UMF-norm.

4. De via het ESP gegeven zoekopdracht heeft tot gevolg dat het EES, [het ETIAS], het VIS, het SIS, Eurodac, [het ECRIS-TCN], het CIR en de MID, alsmede de gegevens van Europol en de databanken van Interpol de gegevens verstrekken die zij bevatten.

5. Wat het doorzoeken van de databanken van Interpol betreft, wordt het ESP zodanig ontworpen dat de gegevens aan de hand waarvan de ESP-gebruiker een zoekopdracht geeft, niet worden gedeeld met de eigenaars van de gegevens van Interpol.

6. Het antwoord aan de ESP-gebruiker is uniek en bevat alle gegevens waartoe de gebruiker op grond van het Unierecht toegang heeft. In voorkomend geval wordt in het door het ESP verstrekte antwoord vermeld van welk informatiesysteem of van welke databank de gegevens deel uitmaken.

7. De Commissie stelt overeenkomstig artikel 63 een gedelegeerde handeling vast met specificaties voor de inhoud en het format van de ESP-antwoorden.

Artikel 10
Bijhouden van logbestanden

1. Onverminderd [artikel 39 van de Eurodac-verordening], [de artikelen 12 en 18 van de SIS-verordening op het gebied van rechtshandhaving], [artikel 29 van de ECRIS-TCN-verordening] en artikel 40 van Verordening (EU) 2016/794 houdt eu-LISA logbestanden bij van alle gegevensverwerkingsverrichtingen in het ESP. In deze logbestanden wordt met name het volgende vermeld:

   (a) de autoriteit van de lidstaat en de individuele ESP-gebruiker, met inbegrip van het gebruikte ESP-profiel bedoeld in artikel 8;

   (b) de datum en het tijdstip van de zoekopdracht;

   (c) de doorzochte EU-informatiesystemen en gegevens van Europol;

   (d) overeenkomstig de nationale regels of Verordening (EU) 2016/794 of in voorkomend geval Verordening (EU) nr. 45/2001, het identificatiekenmerk van de persoon die de zoekopdracht heeft verricht.

2. De logbestanden worden uitsluitend gebruikt voor het toezicht op de gegevensbescherming, onder meer door de toelaatbaarheid van een verzoek en de wettigheid van de gegevensverwerking te controleren, en voor het verzekeren van de gegevensbeveiliging in de zin van artikel 42. De logbestanden worden met passende maatregelen tegen ongeoorloofde toegang beschermd en één jaar na het aanleggen ervan gewist, tenzij zij nodig zijn voor reeds aangevangen toezichtprocedures.

Artikel 11

Vangnetprocedures voor wanneer het Europees zoekportaal om technische redenen niet kan worden gebruikt

1. Indien het ESP vanwege een interne technische storing niet kan worden gebruikt om een of meer van de in artikel 9, lid 1, genoemde EU-informatiesystemen of het CIR te doorzoeken, brengt eu-LISA de ESP-gebruikers daarvan op de hoogte.

2. Indien het ESP vanwege een technische storing in de nationale infrastructuur van een lidstaat niet kan worden gebruikt om een of meer van de in artikel 9, lid 1, genoemde EU-informatiesystemen of het CIR te doorzoeken, brengt de bevoegde autoriteit van die lidstaat eu-LISA en de Commissie daarvan op de hoogte.

3. Tijdens de technische storing is in beide gevallen de in artikel 7, leden 2 en 4, bedoelde verplichting niet van toepassing en kunnen de lidstaten via hun respectieve nationale uniforme interfaces of nationale communicatie-infrastructuur rechtstreeks toegang krijgen tot de in artikel 9, lid 1, bedoelde informatiesystemen of tot het CIR.

HOOFDSTUK III
Gezamenlijke dienst voor biometrische matching

Artikel 12

Gezamenlijke dienst voor biometrische matching

1. Om het CIR en de MID te ondersteunen en de doelstellingen van het EES, het VIS, Eurodac, het SIS en [het ECRIS-TCN] te bevorderen, wordt een gezamenlijke dienst voor biometrische matching (gezamenlijke BMS) opgezet, die biometrische templates opslaat en het mogelijk maakt om aan de hand van biometrische gegevens zoekopdrachten in meerdere EU-informatiesystemen uit te voeren.

2. De gezamenlijke BMS bestaat uit:

   (a) een centrale infrastructuur, waarvan een zoekmachine en de opslag voor de in artikel 13 bedoelde gegevens deel uitmaken;

   (b) een beveiligde communicatie-infrastructuur tussen de gezamenlijke BMS, het centrale SIS en het CIR.

3. eu-LISA zorgt voor de ontwikkeling en het technische beheer van de gezamenlijke BMS.

Artikel 13

Opslag van gegevens in de gemeenschappelijke dienst voor biometrische matching

1. In de gezamenlijke BMS worden de biometrische templates opgeslagen die de dienst extraheert uit de volgende biometrische gegevens:

   (a) de gegevens bedoeld in artikel 16, lid 1, onder d), en artikel 17, lid 1, onder b)

en c), van Verordening (EU) 2017/2226;

(b) de gegevens bedoeld in artikel 9, lid 6, van Verordening (EG) nr. 767/2008;

(c) [de gegevens bedoeld in artikel 20, lid 2, onder w) en x), van de SIS-verordening op het gebied van grenscontroles;

(d) de gegevens bedoeld in artikel 20, lid 3, onder w) en x), van de SIS-verordening op het gebied van rechtshandhaving;

(e) de gegevens bedoeld in artikel 4, lid 3, onder t) en u), van de SIS-verordening op het gebied van de terugkeer van illegaal verblijvende onderdanen van derde landen];

(f) [de gegevens bedoeld in artikel 13, onder a), van de Eurodac-verordening;]

(g) [de gegevens bedoeld in artikel 5, lid 1, onder b), en artikel 5, lid 2, van de ECRIS-TCN-verordening.]

2. Elke in de gezamenlijke BMS opgeslagen biometrische template bevat een verwijzing naar de informatiesystemen waarin de overeenkomstige biometrische gegevens zijn opgeslagen.

3. Biometrische templates worden pas in de gezamenlijke BMS opgenomen nadat de gezamenlijke BMS door middel van een automatische kwaliteitscontrole heeft vastgesteld dat de aan een van de informatiesystemen toegevoegde biometrische gegevens voldoen aan een minimumnorm voor gegevenskwaliteit.

4. De opslag van de in lid 1 bedoelde gegevens moet voldoen aan de in artikel 37, lid 2, bedoelde kwaliteitsnormen.

Artikel 14

Doorzoeken van biometrische gegevens met de gezamenlijke dienst voor biometrische matching

Het CIR en het SIS doorzoeken de in het CIR en het SIS opgeslagen biometrische gegevens aan de hand van de in de gezamenlijke BMS opgeslagen biometrische templates. Zoekopdrachten aan de hand van biometrische gegevens worden uitgevoerd overeenkomstig de doelstellingen vastgesteld in deze verordening, de EES-verordening, de VIS-verordening, de Eurodac-verordening, de [SIS-verordeningen] en [de ECRIS-TCN-verordening].

Artikel 15

Bewaring van gegevens in de gezamenlijke dienst voor biometrische matching

De termijn voor de opslag van de in artikel 13 bedoelde gegevens in de gezamenlijke BMS stemt overeen met die voor de opslag van de overeenkomstige biometrische gegevens in het CIR of het SIS.

Artikel 16

Bijhouden van logbestanden

1. Onverminderd [artikel 39 van de Eurodac-verordening], [de artikelen 12 en 18 van de SIS-verordening op het gebied van rechtshandhaving] en [artikel 29 van de ECRIS-TCN-verordening] houdt eu-LISA logbestanden bij van alle gegevensverwerkingsverrichtingen in de gezamenlijke BMS. In deze logbestanden wordt met name het volgende vermeld:

(a) het relaas in verband met het aanmaken en opslaan van de biometrische templates;

(b) een verwijzing naar de EU-informatiesystemen die zijn doorzocht met de in de gezamenlijke BMS opgeslagen biometrische templates;

(c) de datum en het tijdstip van de zoekopdracht;

(d) het soort biometrische gegevens dat is gebruikt om de zoekopdracht te starten;

(e) de duur van de zoekopdracht;

(f) de resultaten van de zoekopdracht en de datum en het tijdstip van het resultaat;

(g) overeenkomstig de nationale regels of Verordening (EU) 2016/794 of in voorkomend geval Verordening (EU) nr. 45/2001, het identificatiekenmerk van de persoon die de zoekopdracht heeft verricht.

2. De logbestanden worden uitsluitend gebruikt voor het toezicht op de gegevensbescherming, onder meer door de toelaatbaarheid van een verzoek en de wettigheid van de gegevensverwerking te controleren, en voor het verzekeren van de gegevensbeveiliging in de zin van artikel 42. De logbestanden worden met passende maatregelen tegen ongeoorloofde toegang beschermd en één jaar na het aanleggen ervan gewist, tenzij zij nodig zijn voor reeds aangevangen toezichtprocedures. De in lid 1, onder a), bedoelde logbestanden worden gewist zodra de gegevens worden gewist.

HOOFDSTUK IV
Gemeenschappelijk identiteitenregister

Artikel 17
Gemeenschappelijk identiteitenregister

1. Er wordt een gemeenschappelijk identiteitenregister (CIR) ingesteld, waarin voor elke in het EES, het VIS, [het ETIAS], Eurodac of [het ECRIS-TCN] geregistreerde persoon een afzonderlijk bestand met de in artikel 18 bedoelde gegevens wordt aangelegd, met als doel de correcte identificatie van in het EES, het VIS, [het ETIAS], Eurodac of [het ECRIS-TCN] geregistreerde personen te vergemakkelijken en te bevorderen, de werking van de MID te ondersteunen en de toegang van rechtshandhavingsinstanties tot niet voor rechtshandhaving bedoelde informatiesystemen op EU-niveau te vergemakkelijken en te stroomlijnen wanneer dat nodig is voor de preventie, het onderzoek, de opsporing of de vervolging van ernstige criminaliteit.

2. Het CIR bestaat uit:

(a) een centrale infrastructuur die in de plaats komt van de centrale systemen van respectievelijk het EES, het VIS, [het ETIAS], Eurodac en [het ECRIS-TCN], voor zover de in artikel 18 bedoelde gegevens in deze centrale infrastructuur worden opgeslagen;

(b) een beveiligd communicatiekanaal tussen het CIR, de lidstaten en de EU-organen die overeenkomstig het Unierecht gebruik mogen maken van het ESP;

(c) een beveiligde communicatie-infrastructuur tussen het CIR, het EES, [het

ETIAS], het VIS, Eurodac, [het ECRIS-TCN] en de centrale infrastructuur van het ESP, de gezamenlijke BMS en de MID.

3. eu-LISA zorgt voor de ontwikkeling en het technische beheer van het CIR.

Artikel 18

De opslag van gegevens in het gemeenschappelijke identiteitenregister

1. In het CIR worden de volgende gegevens – logisch gescheiden – opgeslagen per informatiesysteem waaruit de gegevens afkomstig zijn:

   (a) – (niet van toepassing);

   (b) – (niet van toepassing);

   (c) – (niet van toepassing);

   (d) [de in artikel 13, onder a) tot en met e), g) en h), van de Eurodac-verordening bedoelde gegevens];

   (e) [de in artikel 5, lid 1, onder b), en artikel 5, lid 2, van de ECRIS-TCN-verordening bedoelde gegevens en de volgende in artikel 5, lid 1, onder a), van die verordening bedoelde gegevens: achternaam of familienaam; voornaam/voornamen; geslacht; geboortedatum; plaats en land van geboorte; nationaliteit/nationaliteiten; gender en, indien van toepassing, vroegere namen, pseudoniemen en/of bijnamen.]

2. In het CIR wordt voor elke reeks gegevens, als bedoeld in lid 1, een verwijzing opgenomen naar de informatiesystemen waar de gegevens deel van uitmaken.

3. De opslag van de in lid 1 bedoelde gegevens moet voldoen aan de in artikel 37, lid 2, bedoelde kwaliteitsnormen.

Artikel 19

Toevoeging, wijziging en wissing van gegevens in het gemeenschappelijke identiteitenregister

1. Wanneer gegevens worden toegevoegd, gewijzigd of gewist in Eurodac of [het ECRIS-TCN], worden de overeenkomstige in artikel 18 bedoelde gegevens die zijn opgeslagen in het afzonderlijke CIR-bestand, automatisch toegevoegd, gewijzigd of gewist.

2. Wanneer de MID overeenkomstig de artikelen 32 en 33 een witte of een rode link aanmaakt tussen de gegevens van twee of meer van de EU-informatiesystemen die deel uitmaken van het CIR, maakt het CIR geen nieuw afzonderlijk bestand aan, maar voegt het de nieuwe gegevens toe aan het afzonderlijke bestand waarin de gelinkte gegevens voorkomen.

Artikel 20

Toegang tot het gemeenschappelijke identiteitenregister met het oog op identificatie

1. Een politieautoriteit van een lidstaat kan, mits zij daartoe op grond van nationale wetgevingsmaatregelen als bedoeld in lid 2 is gemachtigd, het CIR doorzoeken aan de hand van de bij een identiteitscontrole genomen biometrische gegevens van een persoon, doch uitsluitend met het oog op de identificatie van die persoon.

Als de zoekopdracht uitwijst dat in het CIR gegevens over die persoon zijn opgeslagen, krijgt de autoriteit van de lidstaat toegang om de in artikel 18, lid 1, bedoelde gegevens te raadplegen.

Wanneer de biometrische gegevens van de persoon niet kunnen worden gebruikt of wanneer het zoeken aan de hand van die gegevens geen resultaat oplevert, wordt gezocht aan de hand van de identiteitsgegevens van de persoon in combinatie met gegevens van reisdocumenten, of aan de hand van de door die persoon verstrekte identiteitsgegevens.

2. Lidstaten die gebruik wensen te maken van de in dit artikel bedoelde mogelijkheid, stellen daartoe nationale wetgevingsmaatregelen vast. In deze wetgevingsmaatregelen wordt bepaald welke specifieke doelstellingen met de identiteitscontroles worden nagestreefd in het kader van de in artikel 2, lid 1, onder b) en c), omschreven doelen. Voorts worden in de wetgevingsmaatregelen de bevoegde politieautoriteiten aangewezen en de procedures, voorwaarden en criteria voor deze controles vastgelegd.

Artikel 21

Toegang tot het gemeenschappelijke identiteitenregister met het oog op het detecteren van meerdere identiteiten

1. Wanneer een zoekopdracht in het CIR overeenkomstig artikel 28, lid 4, een gele link oplevert, krijgt de in artikel 29 bedoelde autoriteit die bevoegd is voor de verificatie van meerdere identiteiten, uitsluitend voor die verificatie toegang tot de in het CIR opgeslagen identiteitsgegevens die deel uitmaken van de informatiesystemen die in verband staan met de gele link.

2. Wanneer een zoekopdracht in het CIR overeenkomstig artikel 32 een rode link oplevert, krijgen de in artikel 26, lid 2, bedoelde autoriteiten uitsluitend voor de bestrijding van identiteitsfraude toegang tot de in het CIR opgeslagen identiteitsgegevens die deel uitmaken van de informatiesystemen die in verband staan met de rode link.

Artikel 22

Doorzoeken van het gemeenschappelijke identiteitenregister met het oog op rechtshandhaving

1. De aangewezen autoriteiten van de lidstaten en Europol mogen het CIR raadplegen om terroristische misdrijven of andere ernstige strafbare feiten te voorkomen, op te sporen en te onderzoeken, en om zich ervan te vergewissen of Eurodac gegevens over een bepaalde persoon bevat.

2. De aangewezen autoriteiten van de lidstaten en Europol hebben niet het recht om bij het raadplegen van het CIR voor de in lid 1 bedoelde doeleinden, gegevens te raadplegen die deel uitmaken van [het ECRIS-TCN].

3. Wanneer het CIR naar aanleiding van een zoekopdracht aangeeft dat Eurodac gegevens over de betrokken persoon bevat, verwijst het CIR in zijn antwoord aan de aangewezen autoriteiten van de lidstaten en Europol naar de informatiesystemen die de gegevens bevatten die een match opleveren, als bedoeld in artikel 18, lid 2. Het CIR antwoordt op zodanige wijze dat de beveiliging van de gegevens niet in gevaar wordt gebracht.

4. Volledige toegang tot in de EU-informatiesystemen opgenomen gegevens met het oog op het voorkomen, opsporen en onderzoeken van terroristische misdrijven of andere ernstige strafbare feiten blijft onderworpen aan de voorwaarden en procedures als vastgesteld in de desbetreffende wetgevingsinstrumenten waarbij deze toegang wordt geregeld.

Artikel 23
Bewaring van gegevens in het gemeenschappelijke identiteitenregister

1. De in artikel 18, leden 1 en 2, bedoelde gegevens worden gewist in het CIR overeenkomstig de bepalingen over de bewaring van gegevens als vastgesteld in, respectievelijk, [de Eurodac-verordening] en [de ECRIS-TCN-verordening].

2. De termijn voor de opslag van het afzonderlijke bestand in het CIR stemt overeen met die voor de opslag van de overeenkomstige gegevens in ten minste één van de informatiesystemen waaruit de in het CIR aanwezige gegevens afkomstig zijn. Het aanmaken van een link heeft geen gevolgen voor de bewaringstermijn van elk element van de gelinkte gegevens.

Artikel 24
Bijhouden van logbestanden

1. Onverminderd [artikel 39 van de Eurodac-verordening] en [artikel 29 van de ECRIS-TCN-verordening] houdt eu-LISA overeenkomstig de leden 2, 3 en 4 logbestanden bij van alle gegevensverwerkingsverrichtingen in het CIR.

2. Met betrekking tot de toegang tot het CIR op grond van artikel 20 houdt eu-LISA logbestanden bij van alle gegevensverwerkingsverrichtingen in het CIR. In deze logbestanden wordt met name het volgende vermeld:

   (a) het doel van de toegang dat wordt beoogd door de gebruiker die een zoekopdracht via het CIR geeft;

   (b) de datum en het tijdstip van de zoekopdracht;

   (c) het soort gegevens dat is gebruikt om de zoekopdracht te starten;

   (d) de resultaten van de zoekopdracht;

   (e) overeenkomstig de nationale regels of Verordening (EU) 2016/794 of in voorkomend geval Verordening (EU) nr. 45/2001, het identificatiekenmerk van de persoon die de zoekopdracht heeft verricht.

3. Met betrekking tot de toegang tot het CIR op grond van artikel 21 houdt eu-LISA logbestanden bij van alle gegevensverwerkingsverrichtingen in het CIR. In deze logbestanden wordt met name het volgende vermeld:

   (a) het doel van de toegang dat wordt beoogd door de gebruiker die een zoekopdracht via het CIR geeft;

   (b) de datum en het tijdstip van de zoekopdracht;

   (c) in voorkomend geval, de gegevens die zijn gebruikt om de zoekopdracht te starten;

   (d) in voorkomend geval, de resultaten van de zoekopdracht;

   (e) overeenkomstig de nationale regels of Verordening (EU) 2016/794 of in voorkomend geval Verordening (EU) nr. 45/2001, het identificatiekenmerk van

de persoon die de zoekopdracht heeft verricht.

4. Met betrekking tot de toegang tot het CIR op grond van artikel 22 houdt eu-LISA logbestanden bij van alle gegevensverwerkingsverrichtingen in het CIR. In deze logbestanden wordt met name het volgende vermeld:

   (a) het referentiekenmerk van het nationale bestand;

   (b) de datum en het tijdstip van de zoekopdracht;

   (c) het soort gegevens dat is gebruikt om de zoekopdracht te starten;

   (d) de resultaten van de zoekopdracht;

   (e) de naam van de autoriteit die het CIR raadpleegt;

   (f) overeenkomstig de nationale regels of Verordening (EU) 2016/794 of in voorkomend geval Verordening (EU) nr. 45/2001, het identificatiekenmerk van de functionaris die de zoekopdracht heeft verricht, en van de functionaris die de zoekopdracht heeft gelast.

   De overeenkomstig artikel 51 van Verordening (EU) 2016/679 of artikel 41 van Richtlijn (EU) 2016/680 ingestelde toezichthoudende autoriteit verifieert de logbestanden over deze toegang regelmatig, met tussenpozen van ten hoogste zes maanden, om na te gaan of de procedures en voorwaarden als bedoeld in artikel 22, leden 1, 2 en 3, in acht zijn genomen.

5. Elke lidstaat houdt logbestanden bij van de zoekopdrachten die zijn uitgevoerd door personeelsleden die naar behoren zijn gemachtigd om het CIR overeenkomstig de artikelen 20, 21 en 22 te gebruiken.

6. De in de leden 1 en 5 bedoelde logbestanden worden uitsluitend gebruikt voor het toezicht op de gegevensbescherming, onder meer door de toelaatbaarheid van een verzoek en de wettigheid van de gegevensverwerking te controleren, en voor het verzekeren van de gegevensbeveiliging in de zin van artikel 42. De logbestanden worden met passende maatregelen tegen ongeoorloofde toegang beschermd en één jaar na het aanleggen ervan gewist, tenzij zij nodig zijn voor reeds aangevangen toezichtprocedures.

7. eu-LISA bewaart de logbestanden met het relaas van de in een afzonderlijk bestand opgeslagen gegevens, met het oog op de in lid 6 bedoelde doeleinden. De logbestanden met het relaas van de opgeslagen gegevens worden gewist zodra de gegevens worden gewist.

HOOFDSTUK V
Detector van meerdere identiteiten

Artikel 25
Detector van meerdere identiteiten

1. Om de werking van het CIR te ondersteunen en de doelstellingen van het EES, het VIS, [het ETIAS], Eurodac, het SIS en [het ECRIS-TCN] te bevorderen, wordt een detector van meerdere identiteiten (MID) ingesteld, die zorgt voor het aanmaken en opslaan van links tussen gegevens in de EU-informatiesystemen die zijn opgenomen in het CIR en het SIS, en op basis daarvan meerdere identiteiten detecteert, met als

tweeledig doel de identiteitscontroles te vergemakkelijken en identiteitsfraude te bestrijden.

2. De MID bestaat uit:

   (a) een centrale infrastructuur, waarin links en verwijzingen naar informatiesystemen worden opgeslagen;

   (b) een beveiligde communicatie-infrastructuur om de MID te verbinden met het SIS en de centrale infrastructuur van het ESP en het CIR.

3. eu-LISA zorgt voor de ontwikkeling en het technische beheer van de MID.

Artikel 26
Toegang tot de detector van meerdere identiteiten

1. Met het oog op de in artikel 29 bedoelde manuele identiteitsverificatie wordt toegang tot de in artikel 34 bedoelde, in de MID opgeslagen gegevens verleend aan:

   (a) – (niet van toepassing);

   (b) – (niet van toepassing);

   (c) – (niet van toepassing);

   (d) de autoriteiten die bevoegd zijn om overeenkomstig de Eurodac-verordening een verzoek om internationale bescherming te beoordelen, bij het beoordelen van een nieuw verzoek om internationale bescherming;

   (e) het Sirene-bureau van de lidstaat die een signalering creëert [SIS-verordening op het gebied van rechtshandhaving of SIS-verordening op het gebied van de terugkeer van illegaal verblijvende onderdanen van derde landen];

   (f) [de centrale autoriteiten van de lidstaat van veroordeling, bij het invoeren en bijwerken van de gegevens in het ECRIS-TCN overeenkomstig artikel 5 van de ECRIS-TCN-verordening.]

2. De autoriteiten van de lidstaten en de EU-organen die toegang hebben tot ten minste één EU-informatiesysteem dat is opgenomen in het CIR, of tot het SIS, krijgen toegang tot de in artikel 34, onder a) en b), bedoelde gegevens wanneer sprake is van een rode link als bedoeld in artikel 32.

Artikel 27
Detectie van meerdere identiteiten

1. In het CIR en het CIS wordt een detectie van meerdere identiteiten gestart wanneer:

   (a) – (niet van toepassing);

   (b) – (niet van toepassing);

   (c) – (niet van toepassing);

   (d) [een verzoek om internationale bescherming in Eurodac wordt gecreëerd of bijgewerkt overeenkomstig artikel 10 van de Eurodac-verordening];

   (e) [een signalering van een persoon wordt gecreëerd of bijgewerkt in het SIS overeenkomstig de hoofdstukken VI, VII, VIII en IX van de SIS-verordening op het gebied van rechtshandhaving en artikel 3 van de SIS-verordening op het gebied van de terugkeer van illegaal verblijvende onderdanen van derde

landen];

(f) [een gegevensbestand in het ECRIS-TCN wordt gecreëerd of bijgewerkt overeenkomstig artikel 5 van de ECRIS-TCN-verordening.]

2. Wanneer de gegevens in een informatiesysteem als bedoeld in lid 1 biometrische gegevens bevatten, maken het CIR en het centrale SIS voor de detectie van meerdere identiteiten gebruik van de gezamenlijke BMS. De gezamenlijke BMS maakt een vergelijking tussen de uit nieuwe biometrische gegevens verkregen biometrische templates en de reeds in de gezamenlijke BMS opgenomen biometrische templates om na te gaan of over een bepaalde onderdaan van een derde land reeds gegevens zijn opgeslagen in het CIR of het centrale SIS.

3. Naast de in lid 2 bedoelde procedure maken het CIR en het centrale SIS gebruik van het ESP om de in het CIR en het centrale SIS opgeslagen gegevens te doorzoeken aan de hand van de volgende gegevens:

(a) – (niet van toepassing);

(b) – (niet van toepassing);

(c) – (niet van toepassing);

(d) [achternaam/achternamen; voornaam/voornamen; naam/namen bij geboorte, voorheen gebruikte namen en aliassen; geboortedatum, geboorteplaats, nationaliteit(en) en geslacht als bedoeld in artikel 12 van de Eurodac-verordening];

(e) – (niet van toepassing);

(f) [achternaam/achternamen; voornaam/voornamen; naam/namen bij geboorte, voorheen gebruikte namen en aliassen; geboortedatum, geboorteplaats, nationaliteit(en) en geslacht als bedoeld in artikel 20, lid 3, van de SIS-verordening op het gebied van rechtshandhaving];

(g) [achternaam/achternamen; voornaam/voornamen; naam/namen bij geboorte, voorheen gebruikte namen en aliassen; geboortedatum, geboorteplaats, nationaliteit(en) en geslacht als bedoeld in artikel 4 van de SIS-verordening op het gebied van de terugkeer van illegaal verblijvende onderdanen van derde landen;]

(h) [achternaam (familienaam); voornaam/voornamen; geboortedatum, geboorteplaats, nationaliteit(en) en geslacht als bedoeld in artikel 5, lid 1, onder a), van de ECRIS-TCN-verordening.]

4. De detectie van meerdere identiteiten wordt alleen gestart om gegevens die in een informatiesysteem beschikbaar zijn, te vergelijken met gegevens die in andere informatiesystemen beschikbaar zijn.

Artikel 28

Resultaten van de detectie van meerdere identiteiten

1. Wanneer een zoekopdracht als bedoeld in artikel 27, lid 2 of lid 3, geen treffer oplevert, blijven de in artikel 27, lid 1, bedoelde procedures erop van toepassing overeenkomstig de desbetreffende verordeningen.

2. Wanneer een zoekopdracht als bedoeld in artikel 27, lid 2 of lid 3, een of meer treffers oplevert, maakt het CIR, en in voorkomend geval het SIS, een link aan tussen

de gegevens die zijn gebruikt om de zoekopdracht te starten en de gegevens die tot de treffer hebben geleid.

In het geval van meerdere treffers wordt een link aangemaakt tussen alle gegevens die tot de treffer hebben geleid. Als de gegevens al gelinkt waren, wordt de bestaande link uitgebreid tot de gegevens die zijn gebruikt om de zoekopdracht te starten.

3. Wanneer een zoekopdracht als bedoeld in artikel 27, lid 2 of lid 3, een of meer treffers oplevert en de identiteitsgegevens van de gelinkte bestanden identiek of vergelijkbaar zijn, wordt een witte link aangemaakt overeenkomstig artikel 33.

4. Wanneer een zoekopdracht als bedoeld in artikel 27, lid 2 of lid 3, een of meer treffers oplevert en de identiteitsgegevens van de gelinkte bestanden niet als vergelijkbaar kunnen worden beschouwd, wordt een gele link aangemaakt overeenkomstig artikel 30 en is de in artikel 29 bedoelde procedure van toepassing.

5. De Commissie stelt bij uitvoeringshandeling de procedures vast aan de hand waarvan moet worden bepaald welke identiteitsgegevens als identiek of vergelijkbaar worden beschouwd. Deze uitvoeringshandelingen worden overeenkomstig de in artikel 64, lid 2, bedoelde onderzoeksprocedure vastgesteld.

6. De links worden opgeslagen in het in artikel 34 bedoelde identiteitsbevestigingsbestand.

De Commissie stelt bij uitvoeringshandeling de technische voorschriften vast voor het koppelen van gegevens uit verschillende informatiesystemen. Deze uitvoeringshandelingen worden overeenkomstig de in artikel 64, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 29
Manuele verificatie van meerdere identiteiten

1. Onverminderd lid 2 is de autoriteit die verantwoordelijk is voor de verificatie van meerdere identiteiten:

(a) – (niet van toepassing);

(b) – (niet van toepassing);

(c) – (niet van toepassing);

(d) de autoriteit die een verzoek om internationale bescherming als bedoeld in de Eurodac-verordening beoordeelt, voor treffers die zich voordoen bij de beoordeling van een dergelijk verzoek;

(e) het Sirene-bureau van de lidstaat, voor treffers die zich voordoen bij het creëren van een SIS-signalering overeenkomstig [de SIS-verordening op het gebied van rechtshandhaving of de SIS-verordening op het gebied van de terugkeer van illegaal verblijvende onderdanen van derde landen];

(f) de centrale autoriteiten van de lidstaat van veroordeling, voor treffers die zich voordoen bij het invoeren of bijwerken van de gegevens in het ECRIS-TCN overeenkomstig artikel 5 van [de ECRIS-TCN-verordening].

De MID vermeldt in het identiteitsbevestigingsbestand welke autoriteit verantwoordelijk is voor het verifiëren van meerdere identiteiten.

2. Wanneer een link wordt aangemaakt met gegevens in een hieronder omschreven signalering, wordt het Sirene-bureau van de lidstaat die de signalering heeft gecreëerd, beschouwd als de in het identiteitsbevestigingsbestand bedoelde autoriteit die verantwoordelijk is voor het verifiëren van meerdere identiteiten:

   (a) een signalering van personen die worden gezocht met het oog op aanhouding ten behoeve van overlevering of uitlevering als bedoeld in artikel 26 van [de SIS-verordening op het gebied van rechtshandhaving];

   (b) een signalering van vermiste of kwetsbare personen als bedoeld in artikel 32 van [de SIS-verordening op het gebied van rechtshandhaving];

   (c) een signalering van personen die worden gezocht met het oog op een gerechtelijke procedure als bedoeld in artikel 34 van [de SIS-verordening op het gebied van rechtshandhaving];

   (d) [een signalering inzake terugkeer overeenkomstig de SIS-verordening op het gebied van de terugkeer van illegaal verblijvende onderdanen van derde landen];

   (e) een signalering van personen met het oog op onopvallende controle, ondervragingscontrole of gerichte controle als bedoeld in artikel 36 van [de SIS-verordening op het gebied van rechtshandhaving];

   (f) een signalering van onbekende personen die worden gezocht met het oog op identificatie overeenkomstig het nationale recht en bevraging aan de hand van biometrische gegevens als bedoeld in artikel 40 van [de SIS-verordening op het gebied van rechtshandhaving];

3. De autoriteit die verantwoordelijk is voor het verifiëren van meerdere identiteiten, heeft onverminderd lid 4 toegang tot de betrokken gegevens in het desbetreffende identiteitsbevestigingsbestand en tot de gelinkte identiteitsgegevens in het gemeenschappelijke identiteitenregister en, in voorkomend geval, in het SIS, beoordeelt de verschillende identiteiten, actualiseert de link overeenkomstig de artikelen 31, 32 en 33 en voegt deze onverwijld toe aan het identiteitsbevestigingsbestand.

4. – (niet van toepassing).

5. In het geval van meer dan één link wordt elke link afzonderlijk beoordeeld door de autoriteit die verantwoordelijk is voor het verifiëren van meerdere identiteiten.

6. Als de gegevens die een treffer opleveren, al gelinkt zijn, houdt de autoriteit die verantwoordelijk is voor het verifiëren van meerdere identiteiten, rekening met de bestaande links wanneer zij het aanmaken van nieuwe links beoordeelt.

Artikel 30
Gele link

1. Een link tussen gegevens uit twee of meer informatiesystemen wordt in de volgende gevallen ingedeeld als geel:

   (a) de gelinkte gegevens hebben dezelfde biometrische gegevens maar andere identiteitsgegevens, en de verschillende identiteiten zijn niet manueel gecontroleerd;

   (b) de gelinkte gegevens hebben andere identiteitsgegevens, en de verschillende

identiteiten zijn niet manueel gecontroleerd.

2. Indien een link overeenkomstig lid 1 is ingedeeld als geel, is de procedure van artikel 29 van toepassing.

Artikel 31
Groene link

1. Een link tussen gegevens van twee of meer informatiesystemen wordt als groen ingedeeld als de gelinkte gegevens niet dezelfde biometrische gegevens maar wel vergelijkbare identiteitsgegevens hebben en volgens de autoriteit die verantwoordelijk is voor de verificatie van meerdere identiteiten, verwijzen naar twee verschillende personen.

2. Wanneer het CIR of het SIS wordt doorzocht en er een groene link bestaat tussen twee of meer van de informatiesystemen die deel uitmaken van het CIR of het SIS, geeft de MID aan dat de identiteitsgegevens van de gelinkte gegevens niet overeenstemmen met dezelfde persoon. Het doorzochte informatiesysteem vermeldt in zijn antwoord alleen de gegevens van de persoon wiens gegevens voor de zoekopdracht zijn gebruikt, zonder een treffer tot stand te brengen voor de gegevens waartussen een groene link bestaat.

Artikel 32
Rode link

1. Een link tussen gegevens van twee of meer informatiesystemen wordt in de volgende gevallen ingedeeld als rood:

   (a) de gelinkte gegevens hebben dezelfde biometrische gegevens maar andere identiteitsgegevens, en verwijzen volgens de autoriteit die verantwoordelijk is voor de verificatie van meerdere identiteiten, onrechtmatig naar dezelfde persoon;

   (b) de gelinkte gegevens hebben vergelijkbare identiteitsgegevens en verwijzen volgens de autoriteit die verantwoordelijk is voor de verificatie van meerdere identiteiten, onrechtmatig naar dezelfde persoon.

2. Wanneer het CIR of het SIS wordt doorzocht en er een rode link bestaat tussen twee of meer van de informatiesystemen die deel uitmaken van het CIR of het SIS, vermeldt de MID in zijn antwoord de in artikel 34 bedoelde gegevens. De follow-up van een rode link verloopt overeenkomstig het Unierecht en het nationaal recht.

3. Wanneer er een rode link wordt aangemaakt tussen gegevens van het EES, het VIS, [het ETIAS], Eurodac of [het ECRIS-TCN], wordt het afzonderlijke bestand dat in het CIR is opgeslagen, bijgewerkt overeenkomstig artikel 19, lid 1.

4. Onverminderd de bepalingen in verband met de behandeling van signaleringen in het SIS als bedoeld in [de SIS-verordeningen op het gebied van grenscontroles, rechtshandhaving en de terugkeer van illegaal verblijvende onderdanen van derde landen], en onverminderd de beperkingen die nodig zijn om de veiligheid en de openbare orde te handhaven, criminaliteit te voorkomen en te waarborgen dat een nationaal onderzoek niet in gevaar wordt gebracht, meldt de autoriteit die verantwoordelijk is voor de verificatie van meerdere identiteiten, in het geval van een

rode link, aan de betrokken persoon dat meerdere onrechtmatige identiteiten zijn geconstateerd.

5. Wanneer een rode link wordt aangemaakt, stelt de autoriteit die verantwoordelijk is voor de verificatie van meerdere identiteiten een referentie ter beschikking van de autoriteiten die verantwoordelijk zijn voor de gelinkte gegevens.

Artikel 33
Witte link

1. Een link tussen gegevens van twee of meer informatiesystemen wordt in de volgende gevallen ingedeeld als wit:

   (a) de gelinkte gegevens hebben dezelfde biometrische gegevens en dezelfde of vergelijkbare identiteitsgegevens;

   (b) de gelinkte gegevens hebben dezelfde of vergelijkbare identiteitsgegevens en ten minste één informatiesysteem heeft geen biometrische gegevens van de persoon;

   (c) de gelinkte gegevens hebben dezelfde biometrische gegevens maar andere identiteitsgegevens, en verwijzen volgens de autoriteit die verantwoordelijk is voor de verificatie van meerdere identiteiten, naar dezelfde persoon die rechtmatig verschillende identiteitsgegevens heeft.

2. Wanneer het CIR of het SIS wordt doorzocht en er een witte link bestaat tussen een of meer van de informatiesystemen die deel uitmaken van het CIR of het SIS, geeft de MID aan dat de identiteitsgegevens van de gelinkte gegevens overeenstemmen met dezelfde persoon. De doorzochte informatiesystemen vermelden in hun antwoord, in voorkomend geval, alle gelinkte gegevens van de persoon en brengen zo een treffer tot stand met de gegevens waartussen een witte link bestaat, indien de autoriteit die de zoekopdracht heeft gestart, overeenkomstig het Unierecht of het nationaal recht toegang heeft tot de gelinkte gegevens.

3. Wanneer er een witte link wordt aangemaakt tussen gegevens van het EES, het VIS, [het ETIAS], Eurodac of [het ECRIS-TCN], wordt het afzonderlijke bestand dat in het CIR is opgeslagen, bijgewerkt overeenkomstig artikel 19, lid 1.

4. Wanneer na een manuele verificatie van meerdere identiteiten een witte link wordt aangemaakt, brengt de autoriteit die verantwoordelijk is voor de verificatie van meerdere identiteiten, de betrokken persoon op de hoogte van de aanwezigheid van afwijkingen tussen diens in verschillende systemen geregistreerde gegevens, en stelt zij een referentie ter beschikking van de autoriteiten die verantwoordelijk zijn voor de gelinkte gegevens – zulks onverminderd de bepalingen in verband met de behandeling van signaleringen in het SIS als bedoeld in [de SIS-verordeningen op het gebied van grenscontroles, rechtshandhaving en de terugkeer van illegaal verblijvende onderdanen van derde landen].

Artikel 34
Identiteitsbevestigingsbestand

Het identiteitsbevestigingsbestand bevat de volgende gegevens:

   (a) de links, met vermelding van de kleur als bedoeld in de artikelen 30 tot en met 33;

(b) een verwijzing naar de informatiesystemen die de gelinkte gegevens bevatten;

(c) een uniek identificatienummer om de gegevens van de betrokken gelinkte bestanden op te vragen uit de informatiesystemen;

(d) in voorkomend geval, de autoriteit die verantwoordelijk is voor de verificatie van meerdere identiteiten.

Artikel 35
Bewaring van gegevens in de detector van meerdere identiteiten

De termijn voor opslag van de identiteitsbevestigingsbestanden en de desbetreffende gegevens, inclusief links, in de MID is niet langer dan die voor de opslag van de gelinkte gegevens die zijn opgeslagen in twee of meer EU-informatiesystemen.

Artikel 36
Bijhouden van logbestanden

1. eu-LISA houdt logbestanden bij van alle gegevensverwerkingsverrichtingen in de MID. In deze logbestanden wordt met name het volgende vermeld:

   (a) het doel waarvoor de gebruiker toegang heeft en diens toegangsrechten;

   (b) de datum en het tijdstip van de zoekopdracht;

   (c) het soort gegevens dat is gebruikt om de zoekopdracht te starten;

   (d) de referentie naar de gelinkte gegevens;

   (e) het relaas van het identiteitsbevestigingsbestand;

   (f) het identificatiekenmerk van de persoon die de zoekopdracht heeft verricht.

2. Elke lidstaat houdt de logbestanden bij van de personeelsleden die naar behoren gemachtigd zijn om de MID te gebruiken.

3. De logbestanden worden uitsluitend gebruikt voor het toezicht op de gegevensbescherming, onder meer door de toelaatbaarheid van een verzoek en de wettigheid van de gegevensverwerking te controleren, en voor het verzekeren van de gegevensbeveiliging in de zin van artikel 42. De logbestanden worden met passende maatregelen tegen ongeoorloofde toegang beschermd en één jaar na het aanleggen ervan gewist, tenzij zij nodig zijn voor reeds aangevangen toezichtprocedures. De logbestanden met het relaas van identiteitsbevestigingsbestand worden gewist zodra de gegevens in het identiteitsbevestigingsbestand worden gewist.

HOOFDSTUK VI
Maatregelen ter ondersteuning van interoperabiliteit

Artikel 37
Gegevenskwaliteit

1. eu-LISA stelt de automatische mechanismen en procedures vast voor het controleren van de kwaliteit van de gegevens die worden opgeslagen in het SIS, Eurodac, [het ECRIS-TCN], de gezamenlijke BMS, het CIR en de MID.

2. eu-LISA stelt gemeenschappelijke indicatoren voor gegevenskwaliteit vast, alsook de minimumkwaliteitsnormen voor de opslag van gegevens in het SIS, Eurodac, [het ECRIS-TCN], de gezamenlijke BMS, het CIR en de MID.

3. eu-LISA brengt regelmatig verslag uit aan de lidstaten over de automatische mechanismen en procedures voor het controleren van de gegevenskwaliteit en over de gemeenschappelijke indicatoren voor gegevenskwaliteit. eu-LISA brengt ook regelmatig verslag uit aan de Commissie over kwesties die zijn geconstateerd en de lidstaten die hierbij zijn betrokken.

4. Bij uitvoeringshandelingen worden nadere bepalingen vastgesteld inzake de automatische mechanismen en procedures voor het controleren van de gegevenskwaliteit, de gemeenschappelijke indicatoren voor gegevenskwaliteit en de minimumkwaliteitsnormen voor de opslag van gegevens in het SIS, Eurodac, [het ECRIS-TCN], de gezamenlijke BMS, het CIR en de MID, met name met betrekking tot biometrische gegevens. Deze uitvoeringshandelingen worden overeenkomstig de in artikel 64, lid 2, bedoelde onderzoeksprocedure vastgesteld.

5. Eén jaar na de vaststelling van de automatische mechanismen en procedures voor het controleren van gegevenskwaliteit en de gemeenschappelijke indicatoren voor gegevenskwaliteit, en vervolgens om het jaar, evalueert de Commissie de prestaties van de lidstaten op het gebied van gegevenskwaliteit en doet zij zo nodig aanbevelingen. De lidstaten dienen bij de Commissie een actieplan in om de in het evaluatieverslag geconstateerde gebreken te verhelpen en brengen verslag over de voortgang van het actieplan uit tot dit volledig is uitgevoerd. De Commissie legt het evaluatieverslag voor aan het Europees Parlement, de Raad, de Europese Toezichthouder voor gegevensbescherming en het Bureau van de Europese Unie voor de grondrechten dat is opgericht bij Verordening (EG) nr. 168/2007 van de Raad[63].

Artikel 38
Universal Message Format (UMF)

1. Hierbij wordt de norm inzake het Universal Message Format (UMF-norm) ingesteld. De UMF-norm definieert bepaalde elementen van de inhoud van grensoverschrijdende informatie-uitwisseling tussen informatiesystemen, autoriteiten en/of organisaties op het gebied van justitie en binnenlandse zaken.

2. Toepassing van de UMF-norm is verplicht bij de ontwikkeling van [Eurodac], [het ECRIS-TCN], het ESP, het CIR, de MID en in voorkomend geval bij de ontwikkeling, door eu-LISA of een ander EU-orgaan, van nieuwe informatie-uitwisselingsmodellen en informatiesystemen op het gebied van justitie en binnenlandse zaken.

3. Toepassing van de UMF-norm is facultatief in het SIS en in bestaande of nieuwe transnationale informatie-uitwisselingsmodellen en informatiesystemen op het gebied van justitie en binnenlandse zaken die worden ontwikkeld door lidstaten of geassocieerde landen.

[63] Verordening (EG) nr. 168/2007 van de Raad van 15 februari 2007 tot oprichting van een Bureau van de Europese Unie voor de grondrechten (PB L 53 van 22.2.2007, blz. 1).

4. De Commissie stelt een uitvoeringshandeling vast voor het vastleggen en ontwikkelen van de in lid 1 bedoelde UMF-norm. Deze uitvoeringshandeling wordt overeenkomstig de in artikel 64, lid 2, bedoelde onderzoeksprocedure aangenomen.

Artikel 39
Centraal register voor rapportage en statistieken

1. Er wordt een centraal register voor rapportage en statistieken (CRRS) ingesteld om de doelstellingen van Eurodac, het SIS en [het ECRIS-TCN] te ondersteunen en om systeemoverschrijdende statistische gegevens en analytische verslagen te genereren voor doeleinden op het gebied van beleid, operationaliteit en gegevenskwaliteit.

2. eu-LISA zorgt op zijn technische locaties voor het opstellen, implementeren en hosten van het CRRS, met daarin de logisch gescheiden gegevens als bedoeld in [artikel 42, lid 8, van de Eurodac-verordening], [artikel 71 van de SIS-verordening op het gebied van rechtshandhaving] en [artikel 30 van de ECRIS-TCN-verordening]. Aan de hand van in het CRRS opgenomen gegevens kunnen geen personen worden geïdentificeerd. Toegang tot het CRRS wordt uitsluitend met het oog op het opstellen van rapporten en statistieken verleend aan de in [artikel 42, lid 8, van de Eurodac-verordening], [artikel 71 van de SIS-verordening op het gebied van rechtshandhaving] en [artikel 30 van de ECRIS-TCN-verordening] bedoelde autoriteiten door middel van een beveiligde toegang via TESTA (trans-Europese diensten voor telematica tussen overheidsdiensten) met toegangscontrole en specifieke gebruikersprofielen.

3. eu-LISA anonimiseert de gegevens en registreert de geanonimiseerde gegevens in het CRRS. Het anonimiseren van de gegevens gebeurt automatisch.

4. Het CRRS bestaat uit:

   (a) een centrale infrastructuur, bestaande uit een gegevensregister waaruit anonieme gegevens kunnen worden opgevraagd;

   (b) een beveiligde communicatie-infrastructuur voor de verbinding van het CRRS met het SIS, Eurodac en [het ECRIS-TCN] en met de centrale infrastructuur van de gezamenlijke BMS, het CIR en de MID.

5. De Commissie stelt bij uitvoeringshandelingen nadere bepalingen vast over de werking van het CRRS, met inbegrip van specifieke waarborgen voor de verwerking van persoonsgegevens overeenkomstig de leden 2 en 3, en veiligheidsvoorschriften voor het register. Deze uitvoeringshandelingen worden overeenkomstig de in artikel 64, lid 2, bedoelde onderzoeksprocedure aangenomen.

HOOFDSTUK VII
Gegevensbescherming

Artikel 40
Verwerkingsverantwoordelijke

1. Met betrekking tot de verwerking van gegevens in de gezamenlijke BMS worden de autoriteiten van de lidstaten die verwerkingsverantwoordelijke zijn voor Eurodac, het SIS en [het ECRIS-TCN] ook als verwerkingsverantwoordelijke in de zin van artikel 4, punt 7, van Verordening (EU) 2016/679 beschouwd met betrekking tot de door

hen in de respectieve systemen ingevoerde biometrische templates die worden verkregen uit de in artikel 13 bedoelde gegevens, en zijn deze autoriteiten verantwoordelijk voor de verwerking van de biometrische templates in de gezamenlijke BMS.

2. Met betrekking tot de verwerking van gegevens in het CIR worden de autoriteiten van de lidstaten die verwerkingsverantwoordelijke zijn voor Eurodac en [het ECRIS-TCN] ook als verwerkingsverantwoordelijke in de zin van artikel 4, punt 7, van Verordening (EU) 2016/679 beschouwd met betrekking tot de in artikel 18 bedoelde gegevens die zij in de respectieve systemen invoeren, en zijn deze autoriteiten verantwoordelijk voor de verwerking van die persoonsgegevens in het CIR.

3. Met betrekking tot de verwerking van gegevens in de MID geldt dat:

   (a) het Europees Grens- en kustwachtagentschap met betrekking tot de verwerking van persoonsgegevens door de centrale ETIAS-eenheid wordt beschouwd als verantwoordelijke voor de verwerking in de zin van artikel 2, punt b), van Verordening (EG) nr. 45/2001.

   (b) de autoriteiten van de lidstaten die toevoegingen of wijzigingen aanbrengen aan de gegevens in het identiteitsbevestigingsbestand ook als verwerkingsverantwoordelijke in de zin van artikel 4, punt 7, van Verordening (EU) 2016/679 worden beschouwd en verantwoordelijk zijn voor de verwerking van de persoonsgegevens in de MID.

Artikel 41
Verwerker

Met betrekking tot de verwerking van persoonsgegevens in het CIR wordt eu-LISA beschouwd als de verwerker in de zin van artikel 2, punt e), van Verordening (EG) nr. 45/2001.

Artikel 42
Beveiliging van de verwerking

1. Zowel eu-LISA als de autoriteiten van de lidstaten zorgen voor de beveiliging van de verwerking van persoonsgegevens uit hoofde van deze verordening. eu-LISA, [de centrale ETIAS-eenheid] en de autoriteiten van de lidstaten werken samen aan taken op het gebied van beveiliging.

2. Onverminderd artikel 22 van Verordening (EG) nr. 45/2001 neemt eu-LISA de nodige maatregelen ter beveiliging van de interoperabiliteitscomponenten en de bijbehorende communicatie-infrastructuur.

3. Met name neemt eu-LISA passende maatregelen, waaronder de vaststelling van een veiligheidsplan, een bedrijfscontinuïteitsplan en een uitwijkplan, om:

   (a) de gegevens fysiek te beschermen, onder meer met noodplannen voor de bescherming van kritieke infrastructuur;

   (b) te voorkomen dat gegevensdragers onrechtmatig worden gelezen, gekopieerd, gewijzigd of verwijderd;

   (c) te voorkomen dat gegevens onrechtmatig worden ingevoerd en dat opgeslagen persoonsgegevens onrechtmatig worden ingezien, gewijzigd of verwijderd;

   (d) te voorkomen dat gegevens onrechtmatig worden verwerkt, gekopieerd,

gewijzigd of verwijderd;

(e) te waarborgen dat personen die toestemming hebben voor toegang tot de interoperabiliteitscomponenten, uitsluitend toegang hebben tot de gegevens waarop hun toegangsbevoegdheid betrekking heeft, en uitsluitend door middel van persoonlijke gebruikersidentiteiten en geheime toegangsprocedures;

(f) te waarborgen dat kan worden nagegaan en vastgesteld aan welke instanties persoonsgegevens mogen worden doorgegeven door middel van datatransmissieapparatuur;

(g) te waarborgen dat kan worden nagegaan en vastgesteld welke gegevens wanneer, door wie en met welk doel in de interoperabiliteitscomponenten zijn verwerkt;

(h) te voorkomen, in het bijzonder door middel van passende versleutelingstechnieken, dat bij de doorgifte van persoonsgegevens vanuit en naar de interoperabiliteitscomponenten of gedurende het transport van gegevensdragers de gegevens onrechtmatig worden gelezen, gekopieerd, gewijzigd of verwijderd;

(i) de doelmatigheid van de in dit lid bedoelde beveiligingsmaatregelen te controleren, en met betrekking tot de interne controle de nodige organisatorische maatregelen te nemen om te waarborgen dat deze verordening wordt nageleefd.

4. Om de verwerking van persoonsgegevens door autoriteiten met recht op toegang tot een of meer interoperabiliteitscomponenten te beveiligen, nemen de lidstaten maatregelen die gelijkwaardig zijn aan die van lid 3 van dit artikel.

Artikel 43
Vertrouwelijkheid van de SIS-gegevens

1. Alle lidstaten passen, in overeenstemming met hun nationaal recht, de voorschriften inzake het beroepsgeheim of een gelijkwaardige geheimhoudingsplicht toe op alle personen en instanties die moeten werken met SIS-gegevens waartoe zij via een of meer interoperabiliteitscomponenten toegang hebben. Deze geheimhoudingsplicht blijft gelden nadat deze personen hun functie of dienstverband hebben beëindigd of de instanties hun werkzaamheden hebben stopgezet.

2. Onverminderd artikel 17 van het Statuut van de ambtenaren en de regeling welke van toepassing is op de andere personeelsleden van de Europese Unie, past eu-LISA adequate voorschriften inzake het beroepsgeheim of een gelijkwaardige geheimhoudingsplicht toe op alle personen die met SIS-gegevens moeten werken, aan de hand van normen die vergelijkbaar zijn met die van lid 1. Deze geheimhoudingsplicht blijft gelden nadat de personen hun functie of dienstverband hebben beëindigd of hun werkzaamheden hebben stopgezet.

Artikel 44
Beveiligingsincidenten

1. Elke gebeurtenis die gevolgen heeft of kan hebben voor de beveiliging van de interoperabiliteitscomponenten en kan leiden tot beschadiging of verlies van gegevens die in de componenten zijn opgeslagen, wordt beschouwd als een beveiligingsincident, met name wanneer onrechtmatige toegang tot gegevens kan

zijn verkregen of wanneer de beschikbaarheid, integriteit of vertrouwelijkheid van gegevens in gevaar is of kan zijn gekomen.

2. Het beheer van beveiligingsincidenten is gericht op een snelle, doeltreffende en passende reactie.

3. Onverminderd de melding en mededeling van een inbreuk in verband met persoonsgegevens uit hoofde van artikel 33 van Verordening (EU) 2016/679, artikel 30 van Richtlijn (EU) 2016/680, of beide, stellen de lidstaten de Commissie, eu-LISA en de Europese Toezichthouder voor gegevensbescherming in kennis van beveiligingsincidenten. eu-LISA stelt de Commissie en de Europese Toezichthouder voor gegevensbescherming in kennis van beveiligingsincidenten in verband met de centrale infrastructuur van de interoperabiliteitscomponenten.

4. Informatie betreffende een beveiligingsincident dat gevolgen heeft of kan hebben voor de werking van interoperabiliteitscomponenten of voor de beschikbaarheid, integriteit of vertrouwelijkheid van gegevens, wordt aan de lidstaten verstrekt en gerapporteerd in overeenstemming met het door eu-LISA te verstrekken incidentenbeheerplan.

5. De betrokken lidstaten en eu-LISA werken samen wanneer zich een beveiligingsincident voordoet. De Commissie stelt bij uitvoeringshandelingen de specificaties van deze samenwerkingsprocedure vast. Deze uitvoeringshandelingen worden overeenkomstig de in artikel 64, lid 2, bedoelde onderzoeksprocedure aangenomen.

Artikel 45
Interne monitoring

De lidstaten en de betrokken EU-organen zorgen ervoor dat elke autoriteit met recht op toegang tot de interoperabiliteitscomponenten de nodige maatregelen treft met het oog op de naleving van deze verordening en, indien nodig, samenwerkt met de toezichthoudende autoriteit.

De in artikel 40 bedoelde verwerkingsverantwoordelijke neemt de nodige maatregelen, waaronder frequente verificatie van logbestanden, om na te gaan of de gegevens in overeenstemming met deze verordening worden verwerkt, en werkt, indien nodig, samen met de in de artikelen 49 en 50 bedoelde toezichthoudende autoriteiten.

Artikel 46
Recht op informatie

1. Onverminderd het recht op informatie als bedoeld in de artikelen 11 en 12 van Verordening (EG) nr. 45/2001 en de artikelen 13 en 14 van Verordening (EU) 2016/679, worden personen van wie gegevens worden opgeslagen in de gezamenlijke BMS, het CIR of de MID, door de autoriteit die hun gegevens verzamelt, ten tijde van de gegevensverzameling in kennis gesteld van de verwerking van persoonsgegevens met het oog op de toepassing van deze verordening, onder meer met betrekking tot de identiteit en de contactgegevens van de verwerkingsverantwoordelijken, de procedures voor het uitoefenen van hun recht op inzage in en rectificatie of wissing van hun gegevens, alsook de contactgegevens van de Europese Toezichthouder voor gegevensbescherming en van de nationale toezichthoudende autoriteit van de lidstaat die verantwoordelijk is voor het verzamelen van de gegevens.

2. Personen van wie gegevens in Eurodac of [het ECRIS-TCN] worden opgeslagen, worden overeenkomstig lid 1 in kennis gesteld van de verwerking van persoonsgegevens met het oog op de toepassing van deze verordening, wanneer:

(a) – (niet van toepassing);

(b) – (niet van toepassing);

(c) – (niet van toepassing);

(d) [een verzoek om internationale bescherming in Eurodac wordt aangemaakt of bijgewerkt overeenkomstig artikel 10 van de Eurodac-verordening];

(e) [een gegevensbestand in ECRIS-TCN wordt aangemaakt of bijgewerkt overeenkomstig artikel 5 van de ECRIS-TCN-verordening.]

Artikel 47
Recht van inzage, rectificatie en wissing

1. Voor de uitoefening van hun rechten krachtens de artikelen 13 tot en met 16 van Verordening (EG) nr. 45/2001 en de artikelen 15 tot en met 18 van Verordening (EU) 2016/679 heeft elke persoon het recht om zich te wenden tot de lidstaat die verantwoordelijk is voor de manuele verificatie van meerdere identiteiten of tot een andere lidstaat, die het verzoek zal onderzoeken en beantwoorden.

2. De lidstaat die verantwoordelijk is voor de manuele verificatie van meerdere identiteiten als bedoeld in artikel 29, of de aangezochte lidstaat beantwoordt dergelijke verzoeken binnen 45 dagen na ontvangst van het verzoek.

3. Als er een verzoek om rectificatie of wissing van persoonsgegevens wordt gericht tot een andere dan de verantwoordelijke lidstaat, neemt de aangezochte lidstaat binnen zeven dagen contact op met de autoriteiten van de verantwoordelijke lidstaat, die binnen 30 dagen na dit contact de juistheid van de gegevens en de rechtmatigheid van de gegevensverwerking controleren.

4. Wanneer na onderzoek blijkt dat de in de MID opgeslagen gegevens feitelijk onjuist zijn of onrechtmatig zijn geregistreerd, worden deze gegevens gerectificeerd of gewist door de verantwoordelijke lidstaat of, in voorkomend geval, door de aangezochte lidstaat.

5. Wanneer de verantwoordelijke lidstaat tijdens de geldigheidsduur gegevens in de MID wijzigt, bepaalt hij aan de hand van de in artikel 27 en, in voorkomend geval, artikel 29 bedoelde verwerking of een link tussen de gewijzigde gegevens moet worden aangemaakt. Wanneer de verwerking geen treffer oplevert, verwijdert de verantwoordelijke lidstaat of, in voorkomend geval, de aangezochte lidstaat de gegevens uit het identiteitsbevestigingsbestand. Indien de automatische verwerking een of meer treffers oplevert, wordt de link dienovereenkomstig door de verantwoordelijke lidstaat aangemaakt of bijgewerkt overeenkomstig de desbetreffende bepalingen van deze verordening.

6. Indien de verantwoordelijke lidstaat of, in voorkomend geval, de aangezochte lidstaat niet van oordeel is dat de in de MID opgeslagen gegevens feitelijk onjuist zijn of onrechtmatig zijn geregistreerd, stelt die lidstaat een administratief besluit vast waarbij hij de betrokken persoon onverwijld schriftelijk uitlegt waarom hij niet bereid is de gegevens betreffende die persoon te corrigeren of te wissen.

7. Dit besluit informeert de betrokkene tevens over de mogelijkheid om de beslissing inzake het in lid 3 bedoelde verzoek aan te vechten en, indien relevant, over de wijze waarop hij een rechtsvordering kan instellen of een klacht kan indienen bij de bevoegde autoriteiten of rechtbanken, alsmede over bijstand, onder meer van de bevoegde nationale toezichthoudende autoriteiten.

8. Elk verzoek krachtens lid 3 bevat de informatie die nodig is om de betrokkene te identificeren. Deze informatie wordt uitsluitend gebruikt om de uitoefening van de in lid 3 bedoelde rechten mogelijk te maken en wordt onmiddellijk nadien gewist.

9. De verantwoordelijke lidstaat of, in voorkomend geval, de aangezochte lidstaat legt in een schriftelijk document vast dat een in lid 3 bedoeld verzoek is ingediend en op welke wijze dit is behandeld, en stelt dit document onverwijld ter beschikking van de bevoegde nationale toezichthoudende autoriteiten voor gegevensbescherming.

Artikel 48
Mededeling van persoonsgegevens aan derde landen, internationale organisaties en particuliere partijen

Persoonsgegevens die worden opgeslagen in de interoperabiliteitscomponenten of waartoe deze componenten toegang hebben, worden niet doorgegeven aan of ter beschikking gesteld van derde landen, internationale organisaties of particuliere partijen.

Artikel 49
Toezicht door de nationale toezichthoudende autoriteit

1. De krachtens artikel 49 van Verordening 2016/679 aangewezen toezichthoudende autoriteiten zorgen ervoor dat ten minste om de vier jaar een audit van de gegevensverwerkingsverrichtingen van de verantwoordelijke nationale autoriteiten wordt uitgevoerd overeenkomstig de desbetreffende internationale auditnormen.

2. De lidstaten zorgen ervoor dat hun toezichthoudende autoriteit over voldoende middelen beschikt om haar taken uit hoofde van deze verordening te kunnen vervullen.

Artikel 50
Toezicht door de Europese Toezichthouder voor gegevensbescherming

De Europese Toezichthouder voor gegevensbescherming zorgt ervoor dat ten minste om de vier jaar een audit van de activiteiten van eu-LISA op het gebied van de verwerking van persoonsgegevens wordt uitgevoerd overeenkomstig de desbetreffende internationale auditnormen. Een verslag over deze audit wordt toegezonden aan het Europees Parlement, de Raad, eu-LISA, de Commissie en de lidstaten. Voordat de verslagen worden aangenomen, wordt eu-LISA in de gelegenheid gesteld opmerkingen te maken.

Artikel 51
Samenwerking tussen de nationale toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming

1. De Europese Toezichthouder voor gegevensbescherming werkt nauw samen met de nationale toezichthoudende autoriteiten in verband met specifieke kwesties waarvoor nationale betrokkenheid vereist is, met name wanneer de Europese Toezichthouder voor gegevensbescherming of een nationale toezichthoudende autoriteit grote

verschillen tussen praktijken van de lidstaten constateert of potentieel onrechtmatige gegevensdoorgifte via de communicatiekanalen van de interoperabiliteitscomponenten constateert, dan wel in de context van vragen die door een of meer nationale toezichthoudende autoriteiten worden gesteld ten aanzien van de uitvoering en de uitlegging van deze verordening.

2. In de in lid 1 bedoelde gevallen wordt gezorgd voor gecoördineerd toezicht in overeenstemming met artikel 62 van Verordening (EU) 2018/XXXX [herziene Verordening (EG) nr. 45/2001].

HOOFDSTUK VIII
Verantwoordelijkheden

Artikel 52
Verantwoordelijkheden van eu-LISA gedurende de ontwerp- en ontwikkelingsfase

1. eu-LISA zorgt ervoor dat de centrale infrastructuur van de interoperabiliteitscomponenten wordt beheerd in overeenstemming met deze verordening.

2. De interoperabiliteitscomponenten worden door eu-LISA gehost op zijn technische locaties en voorzien in de in deze verordening beschreven functies overeenkomstig de voorwaarden inzake beveiliging, beschikbaarheid, kwaliteit en snelheid bedoeld in artikel 53, lid 1.

3. eu-LISA is verantwoordelijk voor de ontwikkeling van de interoperabiliteitscomponenten en voor alle aanpassingen die nodig zijn met het oog op de interoperabiliteit tussen de centrale systemen van het EES, het VIS, [het ETIAS], het SIS, Eurodac en [ECRIS-TCN], en het ESP, de gezamenlijke BMS, het CIR en de MID.

   Het ontwerp van de fysieke architectuur van de interoperabiliteitscomponenten, met inbegrip van de communicatie-infrastructuur alsook de technische specificaties en de evolutie daarvan met betrekking tot de centrale infrastructuur en de beveiligde communicatie-infrastructuur, wordt door eu-LISA bepaald en na een gunstig advies van de Commissie vastgesteld door de raad van bestuur. eu-LISA verricht ook de nodige aanpassingen van het VIS, Eurodac en [het ECRIS-TCN], als voortvloeiend uit de totstandbrenging van de interoperabiliteit en bedoeld in deze verordening.

   eu-LISA ontwikkelt en implementeert de interoperabiliteitscomponenten zo spoedig mogelijk na de inwerkingtreding van deze verordening en de vaststelling door de Commissie van de maatregelen bedoeld in artikel 8, lid 2, artikel 9, lid 7, artikel 28, leden 5 en 6, artikel 37, lid 4, artikel 38, lid 4, artikel 39, lid 5, en artikel 44, lid 5.

   De ontwikkeling omvat de uitwerking en implementatie van de technische specificaties, het testen en de algehele projectcoördinatie.

4. Gedurende de ontwerp- en ontwikkelingsfase wordt een programmabestuursraad met ten hoogste tien leden ingesteld. Deze raad bestaat uit zeven door de raad van bestuur van eu-LISA uit zijn eigen leden of plaatsvervangers aangewezen leden, de voorzitter van de in artikel 65 bedoelde adviesgroep inzake interoperabiliteit, een door de uitvoerend directeur benoemd lid dat eu-LISA vertegenwoordigt, en één door de Commissie benoemd lid. De door de raad van bestuur van eu-LISA

aangewezen leden worden bij uitsluiting gekozen uit de lidstaten die ten volle gebonden zijn door de wetgeving van de Unie betreffende de ontwikkeling, de oprichting, de exploitatie en het gebruik van de door eu-LISA beheerde grootschalige IT-systemen, en die aan de interoperabiliteitscomponenten zullen deelnemen.

5. De programmabestuursraad komt op gezette tijden, en ten minste driemaal per kwartaal, bijeen. Hij zorgt voor een passend beheer van de fasen waarin de interoperabiliteitscomponenten worden ontworpen en ontwikkeld.

De programmabestuursraad brengt maandelijks schriftelijk verslag over de voortgang van het project uit aan de raad van bestuur. De programmabestuursraad heeft geen beslissingsbevoegdheid of mandaat om de leden van de raad van bestuur van eu-LISA te vertegenwoordigen.

6. De raad van bestuur van eu-LISA stelt het reglement van de programmabestuursraad op, dat met name regels bevat inzake:

(a) het voorzitterschap;

(b) de plaats van vergadering;

(c) de voorbereiding van vergaderingen;

(d) de toelating van deskundigen tot de vergaderingen;

(e) communicatieplannen die zorgen voor volledige informatievoorziening aan de niet-deelnemende leden van de raad van bestuur.

Het voorzitterschap wordt bekleed door een lidstaat die ten volle is gebonden door de wetgeving van de Unie betreffende de ontwikkeling, de oprichting, de exploitatie en het gebruik van de door eu-LISA beheerde grootschalige IT-systemen.

Alle door de leden van de programmabestuursraad gemaakte reis- en verblijfkosten worden betaald door eu-LISA en artikel 10 van het reglement van orde van eu-LISA is van overeenkomstige toepassing. Het secretariaat van de programmabestuursraad wordt verzorgd door eu-LISA.

Tot de ingebruikneming van de interoperabiliteitscomponenten komt de in artikel 65 bedoelde adviesgroep inzake interoperabiliteit op gezette tijden bijeen. Zij brengt na elke bijeenkomst verslag uit aan de programmabestuursraad. Zij ondersteunt de programmabestuursraad met technische deskundigheid en houdt de voortgang van de voorbereidingen van de lidstaten bij.

Artikel 53
Verantwoordelijkheden van eu-LISA na de ingebruikneming

1. Na de ingebruikneming van elke interoperabiliteitscomponent is eu-LISA verantwoordelijk voor het technisch beheer van de centrale infrastructuur en de nationale uniforme interfaces. eu-LISA zorgt in samenwerking met de lidstaten te allen tijde voor de beste beschikbare technologie, onder voorbehoud van een kosten-batenanalyse. eu-LISA is ook verantwoordelijk voor het technisch beheer van de communicatie-infrastructuur als bedoeld in de artikelen 6, 12, 17, 25 en 39.

Het technisch beheer van de interoperabiliteitscomponenten omvat alle taken die nodig zijn om de interoperabiliteitscomponenten zeven dagen per week en 24 uur per dag overeenkomstig deze verordening te laten functioneren, met name de onderhoudswerkzaamheden en technische ontwikkelingen die nodig zijn voor een bevredigende technische kwaliteit van de interoperabiliteitscomponenten, in het

bijzonder wat betreft de tijd die nodig is voor raadpleging van de centrale infrastructuur overeenkomstig de technische specificaties.

2. Onverminderd artikel 17 van het Statuut van de ambtenaren van de Europese Unie past eu-LISA passende voorschriften inzake het beroepsgeheim of een gelijkwaardige geheimhoudingsplicht toe op alle personeelsleden die moeten werken met in de interoperabiliteitscomponenten opgeslagen gegevens. Deze geheimhoudingsplicht blijft ook gelden nadat deze personeelsleden hun functie of dienstverband hebben beëindigd of hun werkzaamheden hebben stopgezet.

3. eu-LISA ontwikkelt en onderhoudt een mechanisme en procedures voor het uitvoeren van kwaliteitscontroles op de in de gezamenlijke BMS en het CIR opgeslagen gegevens overeenkomstig artikel 37.

4. eu-LISA verricht ook taken met betrekking tot het aanbieden van opleiding in het technische gebruik van de interoperabiliteitscomponenten.

Artikel 54
Verantwoordelijkheden van de lidstaten

1. Elke lidstaat is verantwoordelijk voor:

   (a) de aansluiting op de communicatie-infrastructuur van het ESP en het CIR;

   (b) de integratie van de bestaande nationale systemen en infrastructuur met het ESP, de gezamenlijke BMS, het CIR en de MID;

   (c) de organisatie, het beheer, de werking en het onderhoud van de bestaande nationale infrastructuur en de aansluiting daarvan op de interoperabiliteitscomponenten;

   (d) het beheer en de regelingen op grond waarvan de naar behoren gemachtigde personeelsleden van de bevoegde nationale autoriteiten overeenkomstig deze verordening toegang hebben tot het ESP, het CIR en de MID, en de opstelling en regelmatige bijwerking van een lijst van de betrokken personeelsleden en hun profiel;

   (e) de vaststelling van de in artikel 20, lid 3, bedoelde wettelijke maatregelen om toegang te krijgen tot het CIR voor identificatiedoeleinden;

   (f) de manuele verificatie van meerdere identiteiten, als bedoeld in artikel 29;

   (g) de toepassing van de vereisten inzake gegevenskwaliteit op de EU-informatiesystemen en de interoperabiliteitscomponenten;

   (h) het verhelpen van tekortkomingen die zijn geconstateerd in het evaluatieverslag van de Commissie over de gegevenskwaliteit als bedoeld in artikel 37, lid 5.

2. Elke lidstaat sluit zijn in artikel 4, punt 24, bedoelde aangewezen autoriteiten aan op het CIR.

Artikel 54 bis
Verantwoordelijkheden van Europol

1. Europol verwerkt de opdrachten die het ESP geeft om de gegevens van Europol te doorzoeken, en past zijn Quest-interface ("Querying Europol Systems") aan voor gebruik met gegevens waarop het basisbeschermingsniveau van toepassing is.

2. Europol is verantwoordelijk voor het beheer en de regelingen op grond waarvan zijn naar behoren gemachtigde personeelsleden overeenkomstig deze verordening toegang tot het ESP en het CIR hebben en het ESP en het CIR gebruiken, alsmede voor de opstelling en regelmatige bijwerking van een lijst van de betrokken personeelsleden en hun profiel.

Artikel 55
Verantwoordelijkheden van de centrale ETIAS-eenheid

De centrale ETIAS-eenheid is verantwoordelijk voor:

(a) de manuele verificatie van meerdere identiteiten als bedoeld in artikel 29;

(b) het uitvoeren van een detectie van meerdere identiteiten aan de hand van de gegevens die zijn opgeslagen in het VIS, Eurodac en het SIS als bedoeld in artikel 59.

HOOFDSTUK IX
Slotbepalingen

Artikel 56
Verslagen en statistieken

1. De naar behoren gemachtigde personeelsleden van de bevoegde autoriteiten van de lidstaten, van de Commissie en van eu-LISA mogen, uitsluitend met het oog op het opstellen van verslagen en statistieken en zonder dat daarbij personen kunnen worden geïdentificeerd, de volgende gegevens inzake het ESP raadplegen:

   (a) het aantal zoekopdrachten per persoon die het ESP-profiel gebruikt;

   (b) – (niet van toepassing).

2. De naar behoren gemachtigde personeelsleden van de bevoegde autoriteiten van de lidstaten, van de Commissie en van eu-LISA mogen, uitsluitend met het oog op het opstellen van verslagen en statistieken en zonder dat daarbij personen kunnen worden geïdentificeerd, de volgende gegevens inzake het CIR raadplegen:

   (a) het aantal zoekopdrachten als bedoeld in de artikelen 20, 21 en 22;

   (b) nationaliteit, geslacht en geboortejaar van de betrokken persoon;

   (c) het soort reisdocument en de drielettercode van het land dat het reisdocument heeft afgegeven;

   (d) het aantal met en zonder biometrische gegevens uitgevoerde zoekopdrachten.

3. De naar behoren gemachtigde personeelsleden van de bevoegde autoriteiten van de lidstaten, van de Commissie en van eu-LISA mogen, uitsluitend met het oog op het opstellen van verslagen en statistieken en zonder dat daarbij personen kunnen worden geïdentificeerd, de volgende gegevens inzake de MID raadplegen:

   (a) nationaliteit, geslacht en geboortejaar van de betrokken persoon;

   (a) het soort reisdocument en de drielettercode van het land dat het reisdocument heeft afgegeven;

(b) het aantal met en zonder biometrische gegevens uitgevoerde zoekopdrachten;

(c) het aantal en het type links.

4. De naar behoren gemachtigde personeelsleden van het Europees Grens- en kustwachtagentschap, opgericht bij Verordening (EU) 2016/1624 van het Europees Parlement en de Raad[64], hebben toegang om de in de leden 1, 2 en 3 bedoelde gegevens te raadplegen, teneinde risico- en kwetsbaarheidsbeoordelingen zoals bedoeld in de artikelen 11 en 13 van die verordening te kunnen uitvoeren.

5. Voor de toepassing van lid 1 slaat eu-LISA de in lid 1 bedoelde gegevens op in het in hoofdstuk VII behandelde CRRS. De in het CRRS opgenomen gegevens worden niet gebruikt om personen te identificeren, maar om de in lid 1 bedoelde autoriteiten in staat te stellen op maat gesneden verslagen en statistieken op te stellen met als doel de grenscontroles doeltreffender te maken, de autoriteiten te helpen bij de verwerking van visumaanvragen en een op feiten gebaseerde beleidsvorming inzake migratie en veiligheid in de Unie te ondersteunen.

Artikel 57
Overgangsperiode voor het gebruik van het Europees zoekportaal

Gedurende een periode van twee jaar vanaf de ingebruikneming van het ESP zijn de verplichtingen als bedoeld in artikel 7, leden 2 en 4, niet van toepassing en is het gebruik van het ESP facultatief.

Artikel 58
Overgangsperiode voor toepassing van de bepalingen inzake de toegang tot het gemeenschappelijke identiteitenregister voor rechtshandhavingsdoeleinden

Artikel 22 is van toepassing vanaf de datum van ingebruikneming als bedoeld in artikel 62, lid 1.

Artikel 59
Overgangsperiode voor de detectie van meerdere identiteiten

1. Gedurende een periode van één jaar nadat eu-LISA de voltooiing van de test van de MID als bedoeld in artikel 62, lid 1, onder b), heeft gemeld en voordat de MID in gebruik wordt genomen, is de centrale ETIAS-eenheid bedoeld in [artikel 33, onder a), van Verordening (EU) 2016/1624] verantwoordelijk voor het uitvoeren van een detectie van meerdere identiteiten aan de hand van de gegevens die zijn opgeslagen in het VIS, Eurodac en het SIS. Voor de detectie van meerdere identiteiten wordt uitsluitend gebruik gemaakt van biometrische gegevens als bedoeld in artikel 27, lid 2, van deze verordening.

2. Wanneer een zoekopdracht een of meer treffers oplevert en de identiteitsgegevens van de gelinkte bestanden identiek of vergelijkbaar zijn, wordt een witte link aangemaakt overeenkomstig artikel 33.

Wanneer een zoekopdracht een of meer treffers oplevert en de identiteitsgegevens van de gelinkte bestanden niet als vergelijkbaar kunnen worden beschouwd, wordt

[64] Verordening (EU) 2016/1624 van het Europees Parlement en de Raad van 14 september 2016 betreffende de Europese grens- en kustwacht, tot wijziging van Verordening (EU) 2016/399 van het Europees Parlement en de Raad en tot intrekking van Verordening (EG) nr. 863/2007 van het Europees Parlement en de Raad, Verordening (EG) nr. 2007/2004 van de Raad en Besluit 2005/267/EG van de Raad (PB L 251 van 16.9.2016, blz. 1).

een gele link aangemaakt overeenkomstig artikel 30 en is de in artikel 29 bedoelde procedure van toepassing.

In het geval van meerdere treffers wordt een link aangemaakt tussen alle gegevenselementen die tot de treffer hebben geleid.

3. Wanneer een gele link wordt aangemaakt overeenkomstig lid 3, verleent de MID de centrale ETIAS-eenheid toegang tot de identiteitsgegevens in de verschillende informatiesystemen.

4. Wanneer een link wordt aangemaakt met een signalering in het SIS, tenzij deze signalering een weigering van toegang of een als verloren, gestolen of ongeldig gemaakt reisdocument betreft als bedoeld in respectievelijk artikel 24 van de SIS-verordening op het gebied van grenscontroles en artikel 38 van de SIS-verordening op het gebied van rechtshandhaving, verleent de MID aan het Sirene-bureau van de lidstaat die de signalering heeft gecreëerd, toegang tot de identiteitsgegevens in de verschillende informatiesystemen.

5. De centrale ETIAS-eenheid of het Sirene-bureau van de lidstaat die de signalering heeft gecreëerd, heeft toegang tot de gegevens in het identiteitsbevestigingsbestand, maakt een beoordeling van de verschillende identiteiten, werkt de link bij overeenkomstig de artikelen 31, 32 en 33 en voegt deze toe aan het identiteitsbevestigingsbestand.

6. Waar nodig helpt eu-LISA de centrale ETIAS-eenheid bij het uitvoeren van de detectie van meerdere identiteiten als bedoeld in dit artikel.

Artikel 60
Kosten

1. De kosten in verband met de instelling en de werking van het ESP, de gezamenlijke BMS, het CIR en de MID komen ten laste van de algemene begroting van de Unie.

2. De kosten in verband met de integratie van de bestaande nationale infrastructuur, de aansluiting van die infrastructuur op de nationale uniforme interfaces en het hosten van de nationale uniforme interfaces komen ten laste van de algemene begroting van de Unie.

   De volgende kosten komen niet in aanmerking:

   (a) de dienst voor projectbeheer van de lidstaten (vergaderingen, missies, kantoren);

   (b) het hosten van nationale IT-systemen (ruimte, implementatie, elektriciteit, koeling);

   (c) het beheer van nationale IT-systemen (operatoren en contracten voor ondersteuning);

   (d) ontwerp, ontwikkeling, implementatie, beheer en onderhoud van nationale communicatienetwerken.

3. De kosten die worden gemaakt door de aangewezen autoriteiten als bedoeld in artikel 4, punt 24, worden respectievelijk door iedere lidstaat en door Europol gedragen. De kosten voor de aansluiting van de aangewezen autoriteiten op het CIR worden respectievelijk door iedere lidstaat en door Europol gedragen.

Artikel 61
Kennisgevingen

1. De lidstaten melden aan eu-LISA welke in de artikelen 7, 20, 21 en 26 bedoelde autoriteiten gebruik kunnen maken van of toegang hebben tot het ESP, het CIR en de MID.

   Binnen drie maanden na de ingebruikneming van elke interoperabiliteitscomponent overeenkomstig artikel 62 wordt een geconsolideerde lijst van deze autoriteiten bekendgemaakt in het *Publicatieblad van de Europese Unie*. Wanneer de lijst wordt gewijzigd, maakt eu-LISA eenmaal per jaar een bijgewerkte geconsolideerde versie bekend.

2. eu-LISA stelt de Commissie in kennis van de succesvolle afsluiting van de in artikel 62, lid 1, onder b), bedoelde test.

3. De centrale ETIAS-eenheid stelt de Commissie in kennis van de succesvolle afsluiting van de overgangsmaatregel als bedoeld in artikel 59.

4. De Commissie stelt de lidstaten en het publiek door middel van een permanent bijgewerkte openbare website in kennis van de op grond van lid 1 meegedeelde informatie.

Artikel 62
Ingebruikneming

1. De Commissie stelt de datum vast waarop elke interoperabiliteitscomponent in gebruik wordt genomen, nadat aan de volgende voorwaarden is voldaan:

   (a) de in artikel 8, lid 2, artikel 9, lid 7, artikel 28, leden 5 en 6, artikel 37, lid 4, artikel 38, lid 4, artikel 39, lid 5, en artikel 44, lid 5, bedoelde maatregelen zijn goedgekeurd;

   (b) eu-LISA heeft verklaard dat een uitgebreide test van de betrokken interoperabiliteitscomponent, die eu-LISA samen met de lidstaten heeft uitgevoerd, met succes is afgesloten;

   (c) eu-LISA heeft de technische en wettelijke regelingen om de in artikel 8, lid 1, en in de artikelen 13, 19, 34 en 39 bedoelde gegevens te verzamelen en door te geven, gevalideerd en ter kennisgeving aan de Commissie gezonden;

   (d) de lidstaten hebben de in artikel 61, lid 1, bedoelde kennisgevingen aan de Commissie gedaan;

   (e) wat de MID betreft, heeft de centrale ETIAS-eenheid de Commissie in kennis gesteld als bedoeld in artikel 61, lid 3.

2. De Commissie stelt het Europees Parlement en de Raad in kennis van de resultaten van de overeenkomstig lid 1, onder b), uitgevoerde test.

3. Het in lid 1 bedoelde besluit van de Commissie wordt bekendgemaakt in het *Publicatieblad van de Europese Unie*.

4. De lidstaten en Europol nemen de interoperabiliteitscomponenten in gebruik op de overeenkomstig lid 1 door de Commissie bepaalde datum.

Artikel 63
Uitoefening van de bevoegdheidsdelegatie

1. De bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend onder de in dit artikel neergelegde voorwaarden.

2. De in artikel 8, lid 2, en artikel 9, lid 7, bedoelde bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend voor onbepaalde tijd met ingang van [*de datum van inwerkingtreding van deze verordening*].

3. Het Europees Parlement of de Raad kan de in artikel 8, lid 2, en artikel 9, lid 7, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het wordt van kracht op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie* of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.

4. Vóór de vaststelling van een gedelegeerde handeling raadpleegt de Commissie de door elke lidstaat aangewezen deskundigen overeenkomstig de beginselen die zijn neergelegd in het Interinstitutioneel Akkoord over beter wetgeven van 13 april 2016.

5. Zodra de Commissie een gedelegeerde handeling heeft vastgesteld, doet zij daarvan gelijktijdig kennisgeving aan het Europees Parlement en de Raad.

6. Een overeenkomstig artikel 8, lid 2, en artikel 9, lid 7, vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement noch de Raad daartegen binnen een termijn van twee maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie hebben medegedeeld dat zij daartegen geen bezwaar zullen maken. Op initiatief van het Europees Parlement of de Raad wordt die termijn met [twee maanden] verlengd.

Artikel 64
Comitéprocedure

1. De Commissie wordt bijgestaan door een comité. Dat comité is een comité in de zin van Verordening (EU) nr. 182/2011.

2. Wanneer naar dit lid wordt verwezen, is artikel 5 van Verordening (EU) nr. 182/2011 van toepassing.

Artikel 65
Adviesgroep

eu-LISA richt een adviesgroep op, die het agentschap voorziet van expertise inzake interoperabiliteit, in het bijzonder bij de opstelling van het jaarlijkse werkprogramma en van het jaarlijkse activiteitenverslag. Tijdens de fase waarin de interoperabiliteitscomponenten worden ontworpen en ontwikkeld, is artikel 52, leden 4, 5 en 6, van toepassing.

Artikel 66
Opleiding

eu-LISA vervult taken met betrekking tot opleiding over het technische gebruik van de interoperabiliteitscomponenten overeenkomstig Verordening (EU) nr. 1077/2011.

Artikel 67
Praktische handleiding

De Commissie stelt, in nauwe samenwerking met de lidstaten, eu-LISA en andere betrokken agentschappen, een praktische handleiding ter beschikking voor de implementatie en het beheer van de interoperabiliteitscomponenten. De praktische handleiding bevat technische en operationele richtsnoeren, aanbevelingen en beste praktijken. De praktische handleiding wordt door de Commissie in de vorm van een aanbeveling goedgekeurd.

Artikel 68
Monitoring en evaluatie

1. eu-LISA zorgt voor procedures om de ontwikkeling van de interoperabiliteitscomponenten te monitoren in het licht van de doelstellingen op het gebied van planning en kosten, en om de werking van de interoperabiliteitscomponenten te monitoren in het licht van doelstellingen inzake technische resultaten, kosteneffectiviteit, beveiliging en kwaliteit van de dienstverlening.

2. Uiterlijk [*zes maanden na de inwerkingtreding van deze verordening – OPOCE: voeg de juiste datum in*] en vervolgens om de zes maanden tijdens de fase waarin de interoperabiliteitscomponenten worden ontwikkeld, legt eu-LISA het Europees Parlement en de Raad een verslag voor over de stand van zaken bij de ontwikkeling van de interoperabiliteitscomponenten. Zodra de ontwikkeling is afgerond, wordt bij het Europees Parlement en de Raad een verslag ingediend waarin uitvoerig wordt uiteengezet hoe de doelstellingen, met name op het vlak van planning en kosten, zijn bereikt en waarin eventuele afwijkingen worden gerechtvaardigd.

3. Met het oog op het technisch onderhoud heeft eu-LISA toegang tot de nodige informatie over de in de interoperabiliteitscomponenten uitgevoerde gegevensverwerkingsverrichtingen.

4. Vier jaar na de ingebruikneming van elke interoperabiliteitscomponent en vervolgens om de vier jaar legt eu-LISA aan het Europees Parlement, de Raad en de Commissie een verslag voor over de technische werking en de beveiliging van de interoperabiliteitscomponenten.

5. Eén jaar na elk verslag van eu-LISA stelt de Commissie een algemene evaluatie van de componenten op, met inbegrip van:

   (a) een beoordeling van de toepassing van deze verordening;

   (b) een toetsing van de bereikte resultaten aan de doelstellingen, en een beoordeling van de gevolgen voor de grondrechten;

   (c) een beoordeling van de onverminderde geldigheid van de uitgangspunten voor de interoperabiliteitscomponenten;

   (d) een beoordeling van de beveiliging van de interoperabiliteitscomponenten;

   (e) een beoordeling van alle mogelijke gevolgen, met inbegrip van

disproportionele gevolgen voor de verkeersstroom aan grensdoorlaatposten en gevolgen voor de begroting van de Unie.

In de evaluaties worden zo nodig aanbevelingen opgenomen. De Commissie legt het evaluatieverslag voor aan het Europees Parlement, de Raad, de Europese Toezichthouder voor gegevensbescherming en het Bureau van de Europese Unie voor de grondrechten, dat is opgericht bij Verordening (EG) nr. 168/2007 van de Raad[65].

6. De lidstaten en Europol verstrekken eu-LISA en de Commissie de informatie die nodig is om de in de leden 4 en 5 bedoelde verslagen op te stellen. Deze informatie brengt de werkmethoden niet in gevaar en bevat geen informatie waardoor bronnen, namen van personeelsleden of onderzoeken van de aangewezen autoriteiten worden onthuld.

7. eu-LISA verstrekt de Commissie de informatie die nodig is om de in lid 5 bedoelde evaluaties op te stellen.

8. Elke lidstaat en Europol stellen met inachtneming van de nationaalrechtelijke bepalingen inzake de bekendmaking van gevoelige informatie jaarlijkse verslagen op over de doeltreffendheid van de toegang tot in het CIR opgeslagen gegevens met het oog op rechtshandhaving, en nemen daarin informatie en statistieken op over:

   (a) het exacte doel van de raadpleging, met inbegrip van het soort terroristisch misdrijf of ander ernstig strafbaar feit;

   (b) gegronde redenen voor het gegronde vermoeden dat de verdachte, de overtreder of het slachtoffer onder de Eurodac-verordening valt;

   (c) het aantal verzoeken om toegang tot het CIR voor rechtshandhavingsdoeleinden;

   (d) het aantal en het soort van gevallen die hebben geleid tot succesvolle identificaties;

   (e) de noodzaak en het gebruik van het uitzonderlijk dringend geval, met inbegrip van de gevallen waarin dat dringend karakter niet werd aanvaard bij de verificatie achteraf door het centrale toegangspunt.

   De jaarlijkse verslagen van de lidstaten en van Europol worden aan de Commissie toegezonden vóór 30 juni van het daaropvolgende jaar.

Artikel 69
Inwerkingtreding en toepasselijkheid

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

[65] Verordening (EG) nr. 168/2007 van de Raad van 15 februari 2007 tot oprichting van een Bureau van de Europese Unie voor de grondrechten (PB L 53 van 22.2.2007, blz. 1).

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat overeenkomstig de Verdragen.

Gedaan te Straatsburg,

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

1.2. Betrokken beleidsterrein(en)

1.3. Aard van het voorstel/initiatief

1.4. Doelstelling(en)

1.5. Motivering van het voorstel/initiatief

1.6. Duur en financiële gevolgen

1.7. Beheersvorm(en)

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

2.2. Beheers- en controlesysteem

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarig financieel kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

3.2. Geraamde gevolgen voor de uitgaven

3.2.1. Samenvatting van de geraamde gevolgen voor de uitgaven

3.2.2. Geraamde gevolgen voor de beleidskredieten

3.2.3. Geraamde gevolgen voor de administratieve kredieten

3.2.4. Verenigbaarheid met het huidig meerjarig financieel kader

3.2.5. Bijdragen van derden

3.3. Geraamde gevolgen voor de ontvangsten

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van interoperabiliteit tussen de informatiesystemen van de Europese Unie voor veiligheid, grensbeheer en migratiebeheer.

1.2. Betrokken beleidsterrein(en)

Binnenlandse zaken (titel 18)

1.3. Aard van het voorstel/initiatief

X Het voorstel/initiatief betreft **een nieuwe actie**

☐ Het voorstel/initiatief betreft **een nieuwe actie na een proefproject/een voorbereidende actie**[66]

☐ Het voorstel/initiatief betreft **de verlenging van een bestaande actie**

☐Het voorstel/initiatief betreft **een actie die wordt omgebogen naar een nieuwe actie**

1.4. Doelstelling(en)

1.4.1. De met het voorstel/initiatief beoogde strategische meerjarendoelstelling(en) van de Commissie

Grensbeheer – levens redden en de buitengrenzen beveiligen

Met de interoperabiliteitscomponenten kan de informatie in de bestaande EU-systemen voor veiligheid, grensbeheer en migratiebeheer beter worden benut. Deze maatregelen voorkomen vooral dat dezelfde persoon in verschillende systemen wordt geregistreerd met meerdere identiteiten. Momenteel is de unieke identificatie van een persoon mogelijk binnen één bepaald systeem, maar niet systeemoverschrijdend. Deze situatie kan aanleiding geven tot verkeerde beslissingen door de autoriteiten of kan door malafide reizigers worden misbruikt om hun echte identiteit te verbergen.

Betere informatie-uitwisseling

De voorgestelde maatregelen bieden de rechtshandhavingsdiensten een gestroomlijnd maar tegelijk afgebakend kader voor toegang tot deze gegevens. De bestaande, verschillende voorwaarden voor toegang tot elke verzameling gegevens zouden worden vervangen door één reeks voorwaarden.

1.4.2. Specifieke doelstelling(en) en bijbehorend nummer [ ]

Met de oprichting van de interoperabiliteitscomponenten worden de volgende algemene doelstellingen beoogd:

(a) het beheer van de buitengrenzen verbeteren;

(b) bijdragen tot het voorkomen en bestrijden van irreguliere migratie; en

66 In de zin van artikel 54, lid 2, onder a) of b), van het Financieel Reglement.

(c) bijdragen aan een hoog niveau van veiligheid in de ruimte van vrijheid, veiligheid en recht van de Unie, met inbegrip van handhaving van de openbare orde en veiligheid en vrijwaring van de veiligheid op het grondgebied van de lidstaten.

De met interoperabiliteit nagestreefde doelstellingen worden bereikt door:

a) een correcte identificatie van personen te waarborgen;

b) bij te dragen tot de bestrijding van identiteitsfraude;

c) te zorgen voor betere en geharmoniseerde vereisten inzake gegevenskwaliteit voor de respectieve EU-informatiesystemen;

d) de technische en operationele implementatie van bestaande en toekomstige EU-informatiesystemen door de lidstaten te vergemakkelijken;

e) de voorwaarden inzake gegevensbeveiliging en -bescherming voor de respectieve EU-informatiesystemen strenger, eenvoudiger en uniformer te maken;

f) de voorwaarden voor toegang van rechtshandhavingsinstanties tot het EES, het VIS, het ETIAS en Eurodac eenvoudiger en uniformer te maken;

g) de doelstellingen van het EES, het VIS, het ETIAS, Eurodac, het SIS en het ECRIS-TCN te ondersteunen.

Betrokken ABM/ABB-activiteit(en)

Veiligheid en bescherming van de vrijheden: Interne veiligheid

1.4.3. Verwacht(e) resulta(a)t(en) en gevolg(en)

Vermeld de gevolgen die het voorstel/initiatief zou moeten hebben op de begunstigden/doelgroepen

De algemene doelstellingen van dit initiatief vloeien voort uit twee op het Verdrag gebaseerde doelstellingen:

1. verbeteren van het beheer van de buitengrenzen van het Schengengebied, voortbouwend op de Europese migratieagenda en navolgende mededelingen, waaronder de mededeling over de instandhouding en de versterking van het Schengengebied;

2. bijdragen aan de interne veiligheid van de Europese Unie, voortbouwend op de Europese veiligheidsagenda en de werkzaamheden van de Commissie ter voorbereiding van een echte en doeltreffende veiligheidsunie.

De specifieke doelstellingen van dit interoperabiliteitsinitiatief zijn:

De specifieke doelstellingen van dit voorstel zijn:

1. waarborgen dat de eindgebruikers (met name grenswachters, rechtshandhavingsambtenaren, immigratiefunctionarissen en gerechtelijke autoriteiten) snelle, naadloze, systematische en gecontroleerde toegang hebben tot de informatie die zij nodig hebben om hun taken te verrichten;

2. zorgen voor een oplossing voor het opsporen van gevallen waarin meerdere identiteiten gelinkt zijn aan dezelfde reeks biometrische gegevens, met als dubbel oogmerk enerzijds bonafide personen correct te identificeren en anderzijds identiteitsfraude te bestrijden;

3. gemakkelijker maken voor politiediensten om de identiteit te controleren van onderdanen van derde landen die zich op het grondgebied van een lidstaat bevinden; en

4. vergemakkelijken en stroomlijnen van de toegang van rechtshandhavingsinstanties tot niet voor rechtshandhaving bedoelde informatiesystemen op EU-niveau, waar dit nodig is voor preventie, opsporing, onderzoek of vervolging van zware criminaliteit en terrorisme.

Met het oog op specifieke doelstelling nr. 1 zal het Europees zoekportaal (ESP) worden ontwikkeld.

Met het oog op specifieke doelstelling nr. 2 zal de detector van meerdere identiteiten (MID) worden ingesteld, ondersteund door het gemeenschappelijke identiteitenregister (CIR) en de gezamenlijke dienst voor biometrische matching (gezamenlijke BMS).

Met het oog op specifieke doelstelling nr. 3 zullen gemachtigde ambtenaren voor identificatiedoeleinden toegang krijgen tot het CIR.

Met het oog op doelstelling nr. 4 wordt het CIR uitgerust met een functie voor het markeren van treffers die een toegang in twee fasen tot de grensbeheersystemen mogelijk maakt voor rechtshandhaving.

Om de vier in punt 1.4.2 omschreven doelstellingen te ondersteunen, zal naast deze vier interoperabiliteitscomponenten ook een Universal Message Format (UMF) worden ingesteld als EU-norm voor de ontwikkeling van informatiesystemen op het gebied van justitie en binnenlandse zaken, en komt er een centraal register voor rapportage en statistieken (CRRS).

1.4.4. Resultaat- en effectindicatoren

Indicatoren aan de hand waarvan kan worden nagegaan in hoeverre het voorstel/initiatief is uitgevoerd.

Voor elke voorgestelde maatregel moet de desbetreffende component worden ontwikkeld, en vervolgens worden onderhouden en beheerd.

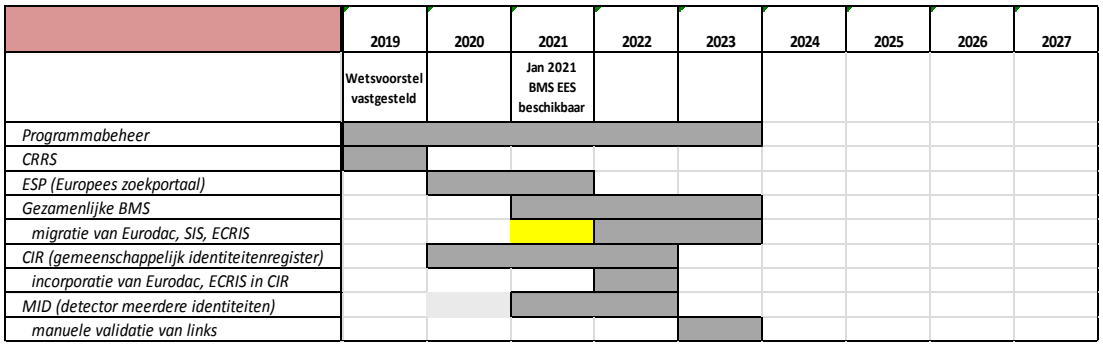
Tijdens de ontwikkeling

Elke component zal worden ontwikkeld zodra de voorwaarden zijn vervuld (d.w.z. het wetgevingsvoorstel is aangenomen door de medewetgevers en de technische voorwaarden zijn vervuld, aangezien sommige componenten pas kunnen worden ontwikkeld wanneer een andere beschikbaar is).

Specifieke doelstelling: bedrijfsklaar tegen de gestelde termijn

Uiterlijk eind 2017 wordt het voorstel ter vaststelling toegezonden aan de medewetgevers. Op basis van de ervaring met het tijdspad voor andere voorstellen wordt aangenomen dat het vaststellingsproces in 2018 zal worden afgerond.

Uitgaande van die veronderstelling wordt begin 2019 (=T0) gehanteerd als startpunt voor de ontwikkeling en als referentiepunt voor de berekening van in duur, en niet in absolute data uitgedrukte perioden. Als de medewetgevers de voorstellen op een later tijdstip vaststellen, verschuift het gehele schema mee. Wel moet in aanmerking worden genomen dat het CIR en de MID pas kunnen worden afgewerkt als de gezamenlijke BMS beschikbaar is. De duur van de ontwikkeling wordt aangeduid op de onderstaande grafiek:



(Het gele blok betreft een specifieke taak in verband met Eurodac.)

- het centrale register voor rapportage en statistieken (CRRS): oplevertermijn: T0 + 12 maanden (2019-2020)

- het Europees zoekportaal (ESP): oplevertermijn: T0 + 36 maanden (2019-2021)

- de gezamenlijke dienst voor biometrische matching (gezamenlijke BMS) wordt eerst ontwikkeld voor de toepassing van het inreis-uitreissysteem (EES). Als dat doel bereikt is, moeten de applicaties die gebruik zullen maken van de gezamenlijke BMS worden geactualiseerd en moeten de gegevens die zijn opgenomen in het geautomatiseerde vingerafdrukidentificatiesysteem van het SIS en van Eurodac en in het ECRIS-TCN, worden gemigreerd naar de gezamenlijke BMS. De oplevertermijn is eind 2023.

- Het gemeenschappelijke identiteitenregister (CIR) wordt eerst ontwikkeld tijdens de tenuitvoerlegging van het EES. Als het EES voltooid is, worden de gegevens uit Eurodac en het ECRIS geïntegreerd in het CIR. De oplevertermijn is eind 2022 (beschikbaarheid van de gezamenlijke BMS + 12 maanden).

- De detector van meerdere identiteiten (MID) wordt ontwikkeld nadat het CIR is gebruik is genomen. De oplevertermijn is eind 2022 (beschikbaarheid van de gezamenlijke BMS + 24 maanden), maar de periode voor het valideren van de links tussen identiteiten die door de MID worden voorgesteld, zal zeer veel middelen vergen. Elke potentiële link moet namelijk manueel worden gevalideerd. Dit werk zal tot eind 2023 duren.

De operationele periode gaat van start zodra de hierboven bedoelde ontwikkelingsperiode is afgelopen.

Operaties

Indicatoren voor elk van de in punt 1.4.3 vermelde specifieke doelstellingen:

1. Specifieke doelstelling: snelle, naadloze en systematische toegang tot geautoriseerde gegevensbronnen

- Het aantal zoekopdrachten dat het ESP kan uitvoeren (*use case executed*) per tijdvak.

- Het aantal door het ESP behandelde zoekopdrachten ten opzichte van het totale aantal zoekopdrachten (via het ESP en rechtstreeks in de systemen), per tijdvak.

2. Specifieke doelstelling: meerdere identiteiten detecteren

- Het aantal aan dezelfde reeks biometrische gegevens gelinkte identiteiten ten opzichte van het aantal identiteiten met biografische informatie, per tijdvak.

- Het aantal geconstateerde gevallen van identiteitsfraude ten opzichte van het aantal gelinkte identiteiten en het totale aantal identiteiten, per tijdvak.

3. Specifieke doelstelling: de identificatie van onderdanen van derde landen bevorderen

- het aantal uitgevoerde identificatiecontroles, ten opzichte van het totale aantal transacties, per tijdvak.

4. Specifieke doelstelling: de toegang tot geautoriseerde gegevensbronnen vereenvoudigen voor rechtshandhavingsdoeleinden

- Het aantal gevallen van "stap 1"-toegang (= controle op de aanwezigheid van gegevens) voor rechtshandhavingsdoeleinden, per tijdvak.

- Het aantal gevallen van "stap 2"-toegang (= daadwerkelijke raadpleging van gegevens in de betrokken EU-systemen) voor rechtshandhavingsdoeleinden, per tijdvak.

5. Overkoepelende, aanvullende doelstelling: de gegevenskwaliteit en het gegevensgebruik verbeteren met het oog op betere beleidsvorming

- Regelmatig uitbrengen van monitoringverslagen over de gegevenskwaliteit.

- Het aantal ad-hocverzoeken om statistische informatie, per tijdvak.

1.5. Motivering van het voorstel/initiatief

1.5.1. Behoefte(n) waarin op korte of lange termijn moet worden voorzien

Zoals blijkt uit de effectbeoordeling bij dit voorstel, zijn de voorgestelde componenten noodzakelijk om interoperabiliteit tot stand te brengen.

• Ter verwezenlijking van de doelstelling om bevoegde gebruikers te voorzien van snelle, naadloze, systematische en gecontroleerde toegang tot relevante informatiesystemen, dient een Europees zoekportaal (ESP) te worden gecreëerd, op basis van een gezamenlijke dienst voor biometrische matching (gezamenlijke BMS) die alle gegevensbanken bestrijkt.

• Ter verwezenlijking van de doelstelling om door gemachtigde ambtenaren verrichte identiteitscontroles van onderdanen van derde landen op het grondgebied van een lidstaat te vergemakkelijken, dient een gemeenschappelijk identiteitenregister (CIR) te worden gecreëerd, met een minimale reeks identificatiegegevens en op basis van dezelfde gezamenlijke BMS.

• Ter verwezenlijking van de doelstelling om meerdere aan dezelfde reeks biometrische gegevens gelinkte identiteiten op te sporen, teneinde zowel identiteitscontroles voor bonafide reizigers te vergemakkelijken als identiteitsfraude te bestrijden, dient een detector van meerdere identiteiten (MID) te worden gebouwd, die links bevat tussen meerdere identiteiten in verschillende systemen.

• Ter verwezenlijking van de doelstelling om de toegang van rechtshandhavingsinstanties tot niet voor rechtshandhaving bedoelde informatiesystemen te vergemakkelijken en stroomlijnen, met het oog op preventie, opsporing, onderzoek of vervolging van zware criminaliteit en terrorisme, dient aan het gemeenschappelijke identiteitenregister (CIR) de mogelijkheid te worden toegevoegd treffers te markeren.

Voor een integrale oplossing die alle doelstellingen haalt, is een combinatie nodig van het ESP, het CIR (met treffermarkering) en de MID, telkens met gebruikmaking van het gezamenlijke BMS.

1.5.2. Toegevoegde waarde van de betrokkenheid van de Unie (deze kan het resultaat zijn van verschillende factoren, o.a. coördinatiewinst, rechtszekerheid, een grotere doeltreffendheid en complementariteit). Voor de toepassing van dit punt wordt onder "toegevoegde waarde van de betrokkenheid van de Unie" verstaan de waarde die een optreden van de Unie oplevert bovenop de waarde die zou zijn gecreëerd indien alleen de lidstaat een maatregel had getroffen.

Optreden op Europees niveau is nodig omdat de systemen die conform de voorstellen interoperabel moeten worden gemaakt, door meerdere lidstaten worden gebruikt: hetzij door alle lidstaten (in het geval van Eurodac), hetzij door alle lidstaten die deel uitmaken van het Schengengebied (in het geval van het EES, het VIS, het ETIAS en het SIS). Per definitie is optreden op een ander niveau uitgesloten.

De belangrijkste verwachte toegevoegde waarde bestaat erin dat een einde wordt gemaakt aan identiteitsfraude, dat in kaart wordt gebracht welke personen meerdere identiteiten hebben gebruikt om de EU binnen te komen en dat bonafide personen niet langer kunnen worden verward met malafide personen met dezelfde naam. Het feit dat de hier voorgestelde interoperabiliteit de implementatie en het onderhoud van de grootschalige IT-systemen van de EU vergemakkelijkt, biedt een extra toegevoegde waarde. De voorgestelde maatregelen moeten de toegang van de rechtshandhavingsdiensten tot specifieke gegevens in grootschalige IT-systemen van de EU bevorderen, zowel qua frequentie als qua resultaat. Op operationeel niveau kan de kwaliteit van de gegevens alleen worden gehandhaafd en verbeterd wanneer deze wordt gemonitord. Voorts moet het, met het oog op beleids- en besluitvorming, mogelijk worden gemaakt om geanonimiseerde gegevens ad hoc te doorzoeken.

Volgens de in het kader van de effectbeoordeling uitgevoerde kosten-batenanalyse kunnen de baten (uitsluitend de kwantificeerbare) redelijkerwijs worden geraamd op ca. 77,5 miljoen EUR per jaar en komen deze met name ten goede aan de lidstaten. De baten houden vooral verband met kostenbesparingen:

- op het gebied van veranderingen aan nationale applicaties wanneer het centrale systeem operationeel is (geraamd op 6 miljoen EUR per jaar voor de IT-afdelingen van de lidstaten);

- omdat wordt gewerkt met een gezamenlijke BMS in plaats van met één BMS per centraal systeem (geraamd op 1,5 miljoen EUR per jaar en een eenmalige kostenbesparing van 8 miljoen EUR voor eu-LISA);

- op het gebied van identificatie van meervoudige identiteiten, in vergelijking met de situatie waarin hetzelfde resultaat zou kunnen worden bereikt zonder de voorgestelde middelen (ten minste 50 miljoen EUR per jaar voor de instanties van de lidstaten bevoegd voor grensbeheer, migratie en rechtshandhaving);

- op het gebied van opleiding voor een grote groep van eindgebruikers, in vergelijking met een situatie waarin periodiek opleiding vereist is (geraamd op 20 miljoen EUR per jaar voor de instanties van de lidstaten bevoegd voor grensbeheer, migratie en rechtshandhaving).

1.5.3. Nuttige ervaring die bij soortgelijke activiteiten in het verleden is opgedaan

Uit de ontwikkeling van het Schengeninformatiesysteem van de tweede generatie (SIS II) en het Visuminformatiesysteem (VIS) zijn de navolgende lessen getrokken.

1. Als mogelijke waarborg tegen kostenoverschrijdingen en vertragingen ten gevolge van veranderende eisen, mogen geen nieuwe informatiesystemen op het gebied van vrijheid, veiligheid en recht worden ontwikkeld, zeker niet als het gaat om een grootschalig IT-systeem, voordat de desbetreffende rechtsinstrumenten waarin het doel, het toepassingsgebied, de functies en de technische details worden beschreven, definitief zijn vastgesteld.

2. Voor het SIS II en het VIS kon de nationale ontwikkeling in de lidstaten medegefinancierd worden uit het Buitengrenzenfonds (EBF), maar dit was niet verplicht. Bijgevolg was het niet mogelijk een volledig beeld te krijgen van de voortgang in de lidstaten die de betrokken activiteiten niet of onvoldoende precies in hun meerjarige programmering hadden opgenomen. Daarom wordt nu voorgesteld dat de Commissie alle door de lidstaten opgelopen integratiekosten terugbetaalt, zodat zij in staat is toe te zien op de voortgang van deze ontwikkelingen.

3. Om de algemene coördinatie van de uitvoering te vergemakkelijken, zal het voorgestelde berichtenverkeer tussen het centrale systeem en de nationale systemen verlopen via bestaande netwerken en de nationale uniforme interface.

1.5.4. Verenigbaarheid en eventuele synergie met andere passende instrumenten

Verenigbaarheid met het huidige meerjarig financieel kader (MFK)

De ISF-grenzenverordening is het financiële instrument waarin het budget voor de uitvoering van het interoperabiliteitsinitiatief is opgenomen.

In artikel 5, lid 5, onder b), is daarom voorzien in een bedrag van 791 miljoen EUR voor de ontwikkeling van IT-systemen gebaseerd op bestaande en/of nieuwe IT-systemen ter beheersing van de migratiestromen langs de buitengrenzen, onder

voorbehoud van de vaststelling van de desbetreffende wetgevingshandelingen van de Unie, en onder de voorwaarden van artikel 15. Van deze 791 miljoen EUR is 480,2 miljoen EUR gereserveerd voor de ontwikkeling van het EES, 210 miljoen EUR voor het ETIAS en 67,9 miljoen EUR voor de herziening van het SIS II. De rest (32,9 miljoen EUR) dient te worden herschikt via de mechanismen van ISF-Grenzen. Binnen de looptijd van het huidige MFK is voor het onderhavige voorstel een bedrag 32,1 miljoen EUR nodig – wat past in het resterende budget.

Voor dit voorstel is in de periode 2019-2027 een budget van in totaal 424,7 miljoen EUR (incl. rubriek 5) vereist. Het lopende MFK dekt enkel 2019 en 2020. Om een onderbouwd beeld te krijgen van de financiële gevolgen van dit voorstel, moet echter een raming van de kosten tot en met 2027 worden opgesteld, zonder vooruit te lopen op het volgende MFK.

Het vereiste budget voor negen jaar bedraagt 424,7 miljoen EUR en omvat ook de volgende posten:

(1) 136,3 miljoen EUR voor de lidstaten, ter dekking van de kosten van de veranderingen in hun nationale systemen voor het gebruik van de interoperabiliteitscomponenten, de door eu-LISA ontwikkelde NUI en de opleiding van de grote groep eindgebruikers. Er is geen effect op het huidige MFK aangezien de financiering pas ingaat in 2021.

(2) 4,8 miljoen EUR voor het Europees Grens- en kustwachtagentschap, voor een team van deskundigen die gedurende één jaar (2023) de links tussen identiteiten zullen valideren wanneer de MID in bedrijf wordt gesteld. Deze activiteiten kunnen worden gerelateerd aan de taken op het gebied van het wegnemen van dubbelzinnigheid over identiteit, die in het ETIAS-voorstel worden toegewezen aan het Europees Grens- en kustwachtagentschap. Er is geen effect op het huidige MFK aangezien de financiering pas ingaat in 2021.

(3) 48,9 miljoen EUR voor Europol, ter dekking van de kosten van de modernisering van zijn IT-systemen met het oog op het te verwerken aantal berichten en ter dekking van de kosten van zijn betere prestaties. De interoperabiliteitscomponenten zullen door het ETIAS worden gebruikt om de gegevens van Europol te raadplegen. De huidige informatieverwerkingscapaciteit van Europol is echter niet afgestemd op de aanzienlijke volumes (gemiddeld 100 000 zoekopdrachten per dag) en de kortere reactietijd. De uitgaven binnen het huidige MFK bedragen 9,1 miljoen EUR.

(4) 2,0 miljoen EUR voor Cepol, voor het voorbereiden en geven van opleidingen aan de operationele personeelsleden. 0,1 miljoen EUR is gepland voor 2020.

(5) 225,0 miljoen EUR voor eu-LISA, ter dekking van de totale kosten voor de ontwikkeling van het programma voor de oplevering van de vijf interoperabiliteitscomponenten (68,3 miljoen EUR), de kosten voor het onderhoud vanaf de oplevering van de componenten tot 2027 (56,1 miljoen EUR), een specifiek budget van 25,0 miljoen EUR voor de migratie van gegevens uit bestaande systemen naar de gezamenlijke BMS, en de extra kosten voor de update van de NUI, het netwerk, opleidingen en vergaderingen. Een specifiek budget van 18,7 miljoen EUR moet de kosten dekken voor het upgraden en beheren van ECRIS-TCN in hogebeschikbaarheidsmodus vanaf 2022. 23,0 miljoen EUR van het totaalbedrag wordt uitgegeven tijdens de looptijd van het huidige MFK.

(6) 7,7 miljoen EUR voor DG HOME, ter dekking van de kosten van een beperkte personeelsuitbreiding en van daarmee samenhangende kosten gedurende de ontwikkelingsfase van de verschillende componenten, aangezien de Commissie gedurende die periode ook de verantwoordelijkheid op zich neemt voor het met het Universal Message Format belaste comité. Dit budget valt onder rubriek 5 en wordt niet gedekt door de ISF-begroting. Voor de periode 2019-2020 is 2,0 miljoen EUR verschuldigd.

Verenigbaarheid met eerdere initiatieven

Dit initiatief is verenigbaar met het volgende.

In april 2016 presenteerde de Commissie een **mededeling over *krachtigere en slimmere informatiesystemen voor grenzen en veiligheid*** om een aantal structurele tekortkomingen in verband met informatiesystemen aan te pakken. Hieruit vloeiden drie maatregelen voort.

Ten eerste nam de Commissie **maatregelen om de voordelen van de bestaande informatiesystemen te versterken en te optimaliseren**. In december 2016 keurde de Commissie voorstellen goed voor de verdere verbetering van het huidige Schengeninformatiesysteem (SIS). In de tussentijd werd, naar aanleiding van het voorstel van de Commissie van mei 2016, het tempo van de onderhandelingen over de herziene rechtsgrondslag voor Eurodac opgevoerd (de EU-databank voor vingerafdrukken in verband met asiel). Ook wordt er gewerkt aan een voorstel voor een nieuwe rechtsgrondslag voor het Visuminformatiesysteem (VIS); dit zal in het tweede kwartaal van 2018 worden ingediend.

In de tweede plaats stelde de Commissie **aanvullende informatiesystemen** voor **om de vastgestelde lacunes** in de EU-architectuur voor gegevensbeheer **op te vullen**. De onderhandelingen over het voorstel van de Commissie van april 2016 tot instelling van een inreis-uitreissysteem (EES)[67] (ter verbetering van de grenscontroleprocedures voor onderdanen van derde landen die naar de EU reizen) werden al in juli 2017 afgerond. De medewetgevers bereikten toen een politiek akkoord, dat in oktober 2017 werd bevestigd door het Europees Parlement en in november 2017 formeel is aangenomen door de Raad. In november 2016 kwam de Commissie met een voorstel tot instelling van een Europees systeem voor reisinformatie en -autorisatie (ETIAS)[68] dat tot doel heeft de veiligheidscontroles van visumvrije reizigers te verscherpen door deze reizigers vooraf te controleren op risico's in verband met irreguliere migratie en veiligheid. De medewetgevers onderhandelen momenteel over dit voorstel. In juni 2017 werd het Europees Strafregister Informatiesysteem voor onderdanen van derde landen (ECRIS-TCN)[69] voorgesteld om de lacune op het gebied van informatie-uitwisseling tussen de lidstaten over veroordeelde onderdanen van derde landen op te vullen

In de derde plaats werkte de Commissie, op basis van de vier opties die in de mededeling[70] van april 2016 werden voorgesteld, toe naar de **interoperabiliteit van de informatiesystemen**. Het ESP, het CIR en de gezamenlijke BMS komen overeen met drie van die vier opties. Later werd duidelijk dat een onderscheid moest worden gemaakt tussen het CIR als databank van identiteiten, en een nieuwe component

67 COM(2016) 194 van 6 april 2016.
68 COM(2016) 731 van 16 november 2016.
69 COM(2017) 344 van 29 juni 2017.
70 COM(2016)205 van 6 april 2016.

(MID) die detecteert dat aan één bepaald biometrische identificatiekenmerk meerdere identiteiten zijn gelinkt. De vier componenten zijn: het ESP, het CIR, de MID en de gezamenlijke BMS.

Synergie

Met "synergie" in dit verband wordt gedoeld op het voordeel dat ontstaat wanneer bestaande oplossingen worden hergebruikt en nieuwe aanvullende investeringen worden voorkomen.

Tussen deze initiatieven en de ontwikkeling van het EES en het ETIAS bestaat een zeer grote mate van synergie.

Voor de werking van het EES wordt een afzonderlijk bestand aangelegd voor alle onderdanen van derde landen die het Schengengebied binnenkomen voor een kort verblijf. Daartoe zal het bestaande biometrische matchingsysteem, dat wordt gebruikt voor het VIS en dat de vingerafdruktemplates voor alle visumplichtige reizigers bevat, worden uitgebreid met de biometrische gegevens van visumvrije reizigers. Conceptueel gezien is de gezamenlijke BMS dus een meer algemene toepassing van het EES-onderdeel dat zal worden gebouwd om biometrische gegevens te matchen. De biometrische templates in het overeenkomstige biometrischematchonderdeel van het SIS en Eurodac zullen vervolgens naar dat gezamenlijke BMS worden "gemigreerd" (d.w.z. overgeheveld van het ene naar het andere systeem). Volgens informatie van de leverancier kost de opslag in aparte databanken gemiddeld 1 EUR per biometrische reeks (potentieel zijn er in totaal 200 miljoen datareeksen) en doet een gezamenlijke BMS de gemiddelde kostprijs dalen tot 0,35 EUR. Deze voordelen worden deels weggestreept door de hogere kosten voor de hardware die nodig is voor een grote hoeveelheid gegevens, maar uiteindelijk vallen de kosten voor een gezamenlijke BMS naar schatting 30 % lager uit dan die voor de opslag van dezelfde data in verschillende kleinere BMS-systemen.

Voor de werking van het ETIAS moet een onderdeel beschikbaar zijn voor het doorzoeken van een reeks EU-systemen. Ofwel wordt hiervoor gebruikgemaakt van het ESP, ofwel wordt een specifieke component gebouwd als onderdeel van het ESP-voorstel. Het interoperabiliteitsvoorstel biedt de mogelijkheid om één component te bouwen in plaats van twee.

Een andere vorm van synergie ligt in het hergebruik van de nationale uniforme interface (NUI) die ook wordt gebruikt voor het EES en het ETIAS. De NUI moet worden bijgewerkt, maar zal in gebruik blijven.

1.6. Duur en financiële gevolgen

☐ Voorstel/initiatief met een **beperkte geldigheidsduur**

– ☐ Voorstel/initiatief is van kracht vanaf [DD/MM]JJJJ tot en met [DD/MM]JJJJ

– ☐ Financiële gevolgen vanaf JJJJ tot en met JJJJ

☒ Voorstel/initiatief met een **onbeperkte geldigheidsduur**

– Ontwikkelingsperiode van 2019 tot en met 2023, gevolgd door een volledige uitvoering.

– Daarom hebben de gegevens over de financiële gevolgen betrekking op de periode van 2019 tot en met 2027.

1.7. Beheersvorm(en)[71]

☒ **Direct beheer** door de Commissie

– X door haar diensten, waaronder het personeel in de delegaties van de Unie;

– ☐ door de uitvoerende agentschappen

☒ **Gedeeld beheer** met lidstaten

☒ **Indirect beheer** door begrotingsuitvoeringstaken te delegeren aan:

– ☐ derde landen of de door hen aangewezen organen;

– ☐ internationale organisaties en hun agentschappen (geef aan welke);

– ☐ de EIB en het Europees Investeringsfonds;

– ☒ de in de artikelen 208 en 209 van het Financieel Reglement bedoelde organen;

– ☐ publiekrechtelijke organen;

– ☐ privaatrechtelijke organen met een openbaredienstverleningstaak, voor zover zij voldoende financiële garanties bieden;

– ☐ privaatrechtelijke organen van een lidstaat, waaraan de uitvoering van een publiek-privaat partnerschap is toevertrouwd en die voldoende financiële garanties bieden;

– ☐ personen aan wie de uitvoering van specifieke maatregelen op het gebied van het GBVB in het kader van titel V van het VEU is toevertrouwd en die worden genoemd in de betrokken basishandeling.

– *Verstrek, indien meer dan een beheersvorm is aangekruist, extra informatie onder "Opmerkingen".*

Opmerkingen

Blokken	Ontwikkelingsfase	Operationele fase	Wijze van beheer	Uitvoerder
Ontwikkeling en onderhoud (van de interoperabiliteitscomponenten voor de centrale systemen,	X	X	Indirect	eu-LISA Europol Cepol

[71] Nadere gegevens over de beheersvormen en verwijzingen naar het Financieel Reglement zijn beschikbaar op BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Blokken	Ontwikkelingsfase	Operationele fase	Wijze van beheer	Uitvoerder
opleiding inzake het systeem)				
Migratie van gegevens (migratie van biometrische templates naar een gezamenlijke BMS), netwerkkosten, update van de NUI, vergaderingen en opleiding	X	X	Indirect	eu-LISA
Validering van links bij het creëren van de MID	X	-	Indirect	Europees Grens- en kustwachtagentschap
Aanpassing van de NUI aan de gebruiker, integratie van de nationale systemen en opleiding van de eindgebruikers	X	X	Gedeeld (of direct) (1)	COM + lidstaten

(1) In dit instrument zijn geen bedragen opgenomen voor de operationele fase.

De ontwikkelingsfase begint in 2019 en duurt tot de oplevering van iedere component, vanaf 2019 tot en met 2023 (zie punt 1.4.4).

1. Direct beheer door DG HOME: tijdens de ontwikkelingsfase kunnen zo nodig ook acties direct door de Commissie worden uitgevoerd. Het kan met name gaan over EU-ondersteuning in de vorm van subsidies (ook voor nationale autoriteiten van lidstaten), overheidsopdrachten en/of de vergoeding van kosten van externe deskundigen.

2. Gedeeld beheer: tijdens de ontwikkelingsfase zullen de lidstaten hun nationale systemen moeten aanpassen om toegang te krijgen tot het ESP in plaats van tot individuele systemen (voor uitgaande berichten) en voor veranderingen in de antwoorden op hun zoekopdrachten (voor inkomende berichten). Voorts zal een update worden verricht van de bestaande NUI die voor het EES en het ETIAS is geïmplementeerd.

3. Indirect beheer: eu-LISA zal de ontwikkeling van alle IT-onderdelen van het project voor zijn rekening nemen, namelijk de interoperabiliteitscomponenten, de update van de NUI in elke lidstaat, de update van de communicatie-infrastructuur tussen het centrale systeem en de nationale uniforme interfaces, de migratie van biometrische templates van het bestaande biometrischematchsysteem van het SIS en Eurodac naar de gezamenlijke BMS en het opschonen van de gegevens dat met deze activiteit gepaard gaat.

Tijdens de operationele fase zal eu-LISA alle technische activiteiten uitvoeren die verband houden met het onderhoud van de componenten.

In het Europees Grens- en kustwachtagentschap zal een extra team de links valideren zodra de MID in gebruik wordt genomen. Deze taak is tijdelijk.

Europol zal de ontwikkeling en het onderhoud van zijn systemen afstemmen op de interoperabiliteit met het ESP en het ETIAS. Cepol zorgt voor het voorbereiden en geven van opleiding aan de operationele diensten volgens de "opleiders opleiden"-aanpak.

2. BEHEERSMAATREGELEN

2.1. Monitoring- en rapportageregels

Vermeld frequentie en voorwaarden.

De monitoring- en rapportageregels voor de ontwikkeling en het onderhoud van andere systemen:

1. eu-LISA zorgt voor procedures om de ontwikkeling van het de interoperabiliteitscomponenten te monitoren in het licht van de doelstellingen op het gebied van planning en kosten, en om de werking van de interoperabiliteitscomponenten te monitoren in het licht van doelstellingen inzake technische resultaten, kosteneffectiviteit, beveiliging en kwaliteit van de dienstverlening.

2. Uiterlijk zes maanden na de inwerkingtreding van deze verordening en vervolgens om de zes maanden tijdens de ontwikkelingsfase, legt eu-LISA het Europees Parlement en de Raad een verslag voor over de stand van zaken van de ontwikkeling van elke component. Zodra de ontwikkeling is afgerond, wordt bij het Europees Parlement en de Raad een verslag ingediend waarin uitvoerig wordt uiteengezet hoe de doelstellingen, met name op het vlak van planning en kosten, zijn bereikt en waarin eventuele afwijkingen worden gerechtvaardigd.

3. Met het oog op het technisch onderhoud heeft eu-LISA toegang tot de nodige informatie over de in de componenten uitgevoerde gegevensverwerkingsverrichtingen.

4. Vier jaar na de ingebruikneming van de laatste component en vervolgens om de vier jaar legt eu-LISA aan het Europees Parlement, de Raad en de Commissie een verslag voor over de technische werking van de componenten.

5. Vijf jaar na de ingebruikneming van de laatste component en vervolgens om de vier jaar stelt de Commissie een algemene evaluatie op en doet zij zo nodig aanbevelingen. Deze algemene evaluatie heeft onder meer betrekking op: de mate waarin de componenten de doelstellingen hebben gehaald, op het gebied van interoperabiliteit, onderhoudbaarheid, prestaties en financiële gevolgen, en de implicaties voor de grondrechten.

De Commissie legt het evaluatieverslag voor aan het Europees Parlement en de Raad.

6. De lidstaten en Europol verstrekken eu-LISA en de Commissie de informatie die nodig is om de in de leden 4 en 5 bedoelde verslagen op te stellen overeenkomstig de vooraf door de Commissie en/of eu-LISA bepaalde kwantitatieve indicatoren. Deze informatie brengt de werkmethoden niet in gevaar en bevat geen informatie waardoor bronnen, de identiteit van personeelsleden of onderzoeken van de aangewezen autoriteiten worden onthuld.

7. eu-LISA verstrekt de Commissie de informatie die nodig is om de in lid 5 bedoelde algemene evaluaties op te stellen.

8. Elke lidstaat en Europol stellen met inachtneming van de nationaalrechtelijke bepalingen inzake de bekendmaking van gevoelige informatie, jaarlijkse verslagen op over de doeltreffendheid van de toegang tot EU-systemen voor rechtshandhavingsdoeleinden, waarin informatie en statistieken zijn opgenomen over het volgende:

- het exacte doel van de raadpleging, met inbegrip van het soort terroristisch misdrijf of ander ernstig strafbaar feit;

- gegronde redenen voor het gegronde vermoeden dat de verdachte, de overtreder of het slachtoffer onder deze verordening valt;

- het aantal verzoeken om toegang tot de componenten voor rechtshandhavingsdoeleinden;

- het aantal en het soort van gevallen die hebben geleid tot succesvolle identificaties;

- de noodzaak en het gebruik van het uitzonderlijk dringend geval, met inbegrip van de gevallen waarin dat dringend karakter niet werd aanvaard bij de verificatie achteraf door het centrale toegangspunt.

De jaarlijkse verslagen van de lidstaten en van Europol worden uiterlijk op 30 juni van het daaropvolgende jaar aan de Commissie toegezonden.

2.2. Beheers- en controlesysteem

2.2.1. Mogelijke risico's

De risico's zijn die welke gepaard gaan met de IT-ontwikkeling van vijf onderdelen door een externe contractant onder het beheer van eu-LISA. Dit zijn typische risico's die aan een dergelijk project zijn verbonden:

1. de termijn voor de afronding van het project wordt overschreden;

2. de begroting voor de afronding van het project wordt overschreden;

3. het project wordt slechts gedeeltelijk voltooid.

Het eerste risico is het belangrijkste omdat kosten doorgaans tijdsgebonden zijn (personeelskosten, jaarlijks verschuldigde licentiekosten, enz.) en vertraging de kosten opdrijft.

Deze risico’s kunnen worden beperkt aan de hand van technieken voor projectbeheer, onder meer door in de ontwikkelingsprojecten en op het vlak van personeel voldoende ruimte te voorzien om pieken in het werk op te vangen. De projectinspanning wordt namelijk meestal geraamd uitgaande van een gelijkelijk over de tijd gespreide werklast, terwijl deze in de werkelijkheid meestal schommelingen vertoont, die worden opgevangen door meer middelen toe te wijzen.

Het werken met een externe contractant bij deze ontwikkelingstaak houdt verscheidene risico's in:

1. met name het risico dat de contractant onvoldoende middelen uittrekt voor het project of een systeem ontwerpt en ontwikkelt dat niet geavanceerd is;

2. het risico dat de contractant de administratieve technieken en methoden voor grootschalige IT-projecten niet geheel in acht neemt om de kosten te drukken;

3. ten slotte het risico dat de contractant in financiële moeilijkheden komt door factoren die los staan van dit project.

Deze risico's worden beperkt door de opdrachten te gunnen op basis van solide kwaliteitscriteria, de referenties van de contractanten te controleren en nauw contact met hen te onderhouden. Ten slotte kunnen voor het uiterste geval strenge sanctie- en contractbeëindigingsclausules worden bedongen en zo nodig toegepast.

2.2.2. Informatie over het ingestelde systeem voor interne controle

eu-LISA moet een expertisecentrum worden op het gebied van de ontwikkeling en het beheer van grootschalige IT-systemen. Het agentschap voert de activiteiten uit die verband houden met de ontwikkeling en het beheer van de verschillende interoperabiliteitscomponenten, met inbegrip van het onderhoud van de nationale uniforme interface in de lidstaten.

Gedurende de ontwikkelingsfase zullen alle ontwikkelingsactiviteiten voor alle onderdelen van het project door eu-LISA worden uitgevoerd. De kosten in verband met de integratie van de systemen in de lidstaten tijdens de ontwikkeling zullen door de Commissie worden beheerd via gedeeld beheer of subsidies.

Tijdens de operationele fase zal eu-LISA verantwoordelijk zijn voor het technisch en financieel beheer van de centraal gebruikte componenten, met name wat de gunning en het beheer van opdrachten betreft. De Commissie zal de voor de lidstaten bestemde middelen voor uitgaven met betrekking tot de nationale eenheden beheren via het ISF-Grenzen (nationale programma's).

Om vertragingen op nationaal niveau te voorkomen, moet voorafgaand aan de ontwikkelingsfase worden gezorgd voor doeltreffende governance tussen alle belanghebbenden. De Commissie gaat ervan uit dat bij de start van het project een interoperabele architectuur wordt gedefinieerd die moet worden toegepast in de EES- en de ETIAS-projecten, aangezien deze projecten aan de basis liggen van en gebruik maken van de gezamenlijke BMS, het gemeenschappelijke identiteitenregister en het Europees zoekportaal. Een lid van het team dat het interoperabiliteitsproject beheert, zou deel moeten uitmaken van de projectbeheerstructuur voor het EES en het ETIAS.

2.2.3. Raming van de kosten en baten van de controles en beoordeling van het verwachte foutenrisico

Er is geen raming verstrekt, aangezien de taak om risico's te beheersen en te beperken per definitie bij de projectbeheerstructuur ligt.

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

Vermeld de bestaande en geplande preventie- en beschermingsmaatregelen.

De fraudebestrijdingsmaatregelen staan in artikel 35 van Verordening (EU) nr. 1077/2011 en houden het navolgende in.

1. Met het oog op de bestrijding van fraude, corruptie en andere onwettige activiteiten is Verordening (EG) nr. 1073/1999 van toepassing.

2. Het agentschap treedt toe tot het Interinstitutioneel Akkoord betreffende de interne onderzoeken verricht door het Europees Bureau voor fraudebestrijding (OLAF) en stelt onverwijld de dienovereenkomstige voorschriften vast, die op alle personeelsleden van het agentschap van toepassing zijn.

3. In de financieringsbesluiten en de uitvoeringsovereenkomsten en -instrumenten die uit die besluiten voortvloeien, wordt uitdrukkelijk bepaald dat de Rekenkamer en OLAF, indien nodig, tot controle ter plaatse kunnen overgaan bij de begunstigden van de middelen van het agentschap en bij de tussenpersonen die deze middelen verdelen.

Overeenkomstig deze bepaling heeft de raad van bestuur van het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht op 28 juni 2012 een besluit vastgesteld over

de voorwaarden voor interne onderzoeken in verband met het voorkomen van fraude, corruptie en alle andere onwettige activiteiten waardoor de financiële belangen van de Europese Unie worden geschaad.

De strategie voor fraudepreventie en -opsporing van DG HOME zal van toepassing zijn.

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

DE IN DIT FINANCIEEL MEMORANDUM OPGENOMEN RAMING VAN DE GEVOLGEN VAN DIT VOORSTEL VOOR DE UITGAVEN EN PERSONELE MIDDELEN VANAF 2021 ZIJN BEDOELD TER ILLUSTRATIE EN DOEN GEEN AFBREUK AAN HET MEERJARIG FINANCIEEL KADER.

3.1. Rubriek(en) van het meerjarig financieel kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

- Bestaande begrotingsonderdelen

In volgorde van de rubrieken van het meerjarig financieel kader en de begrotingsonderdelen

Rubriek van het meerjarig financieel kader	Begrotingsonderdeel	Soort uitgave	Bijdrage			
	Nummer [Rubriek……...……]	GK/NGK[72]	van EVA-landen[73]	van kandidaat-lidstaten[74]	van derde landen	in de zin van artikel 21, lid 2, onder b), van het Financieel Reglement.
3	18.02.01.03 – Slimme Grenzen	GK	Nee	Nee	Ja	Nee
3	18.02.03 – Europees Grens- en kustwachtagentschap (Frontex)	GK	Nee	Nee	Ja	Nee
3	18.02.04 – Europol	GK	Nee	Nee	Nee	Nee
3	18.02.05 – Cepol	NGK	Nee	Nee	Nee	Nee
3	18.02.07 – Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (eu-LISA)	GK	Nee	Nee	Ja	Nee

[72] GK = gesplitste kredieten, NGK = niet-gesplitste kredieten.

[73] EVA: Europese Vrijhandelsassociatie.

[74] Kandidaat-lidstaten en, in voorkomend geval, potentiële kandidaat-lidstaten van de Westelijke Balkan.

3.2. Geraamde gevolgen voor de uitgaven

[Dit deel moet worden ingevuld op de **spreadsheet met administratieve begrotingsgegevens** (tweede document in de bijlage bij dit financieel memorandum), te uploaden in DECIDE met het oog op overleg tussen de diensten.]

3.2.1. Samenvatting van de geraamde gevolgen voor de uitgaven

miljoen EUR (tot op drie decimalen)

Rubriek van het meerjarig financieel kader	3	Veiligheid en burgerschap

DG HOME			Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**	Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**Jaar 2028**	**TOTAAL**
• Beleidskredieten													
18.02.01.03 – Slimme Grenzen	Vastleggingen	(1)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Betalingen	(2)	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300
Uit het budget van specifieke programma's gefinancierde administratieve kredieten[75]													
Nummer begrotingsonderdeel		(3)											
TOTAAL kredieten voor DG HOME	Vastleggingen	=1+1a +3)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Betalingen	=2+2a +3	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300

De uitgaven betreffen:

[75] Technische en/of administratieve bijstand en uitgaven ter ondersteuning van de uitvoering van programma's en/of acties van de EU (vroegere "BA"-onderdelen), onderzoek door derden, eigen onderzoek.

– de kosten voor het aanpassen van de nationale uniforme interface (NUI) die met financiële middelen uit hoofde van het EES-voorstel wordt ontwikkeld, voor het afstemmen van de systemen in de lidstaten op de veranderde centrale systemen, en voor het opleiden van de eindgebruikers.

18.0203 – Europese grens- en kustwacht			Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**	Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**TOTAAL**
Titel 1: personeelsuitgaven	Vastleggingen	(1)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
	Betalingen	(2)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
Titel 2: infrastructuur- en operationele uitgaven	Vastleggingen	(1a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
	Betalingen	(2a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
Titel 3: operationele uitgaven	Vastleggingen	(3a)	0	0	0	0,183	2,200	0	0	0	0	2,383
	Betalingen	(3b)	0	0	0	0,183	2,200	0	0	0	0	2,383
TOTAAL kredieten voor Europol	(totaal vastleggingen = totaal betalingen)	=1+1a +3a	**0**	**0**	**0**	**0,776**	**4,744**	**0,402**	**0**	**0**	**0**	**5,923**

– De begroting voor de Europese grens- en kustwacht (EGKW) omvat de uitgaven voor een team dat de door de MID (detector van meerdere identiteiten) aangemaakte links tussen de bestaande gegevens valideert (min of meer 14 miljoen registraties). Het aantal manueel te valideren links wordt geschat op ca. 550 000.
Vanwege de functioneel nauwe band en om de kosten voor het oprichten van een nieuw team te besparen, wordt dit specifieke team toegevoegd aan het EGKW-team dat is opgezet voor het ETIAS. Dit werk zal waarschijnlijk in 2023 worden uitgevoerd. De contractanten worden uiterlijk drie maanden vooraf aangeworven en hun contracten lopen uiterlijk twee maanden na het einde van de migratie af. Een ander deel van het vereiste personeelsbestand zal niet als contractant worden aangeworven, maar als consultant worden ingehuurd. Dit verklaart de kosten onder titel 3 voor 2023. Deze personen zouden een maand van tevoren worden ingehuurd. Nadere gegevens over het personeelsbestand worden later verstrekt.

– Titel 1 omvat dus de kosten van twintig interne personeelsleden en de begrotingsmiddelen om het leidinggevend en ondersteunend personeel te versterken.

– Titel 2 omvat de extra accommodatiekosten voor de tien extra personeelsleden van de contractant.

– Titel 3 omvat de vergoeding voor de tien extra personeelsleden van de contractant. Er zijn geen andere soorten kosten opgenomen.

18.0204 — Europol			Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**	Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**TOTAAL**
Titel 1: personeelsuitgaven	Vastleggingen	(1)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
	Betalingen	(2)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
Titel 2: infrastructuur- en operationele uitgaven	Vastleggingen	(1a)	0	0	0	0	0	0	0	0	0	0
	Betalingen	(2a)	0	0	0	0	0	0	0	0	0	0
Titel 3: operationele uitgaven	Vastleggingen	(3a)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
	Betalingen	(3b)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
TOTAAL kredieten voor Europol	(totaal vastleggingen = totaal betalingen)	=1+1a +3a	0,690	8,382	8,382	3,589	3,589	3,382	8,732	8,732	3,382	48,860

De uitgaven van Europol omvatten de upgrade van de ICT-systemen van Europol die nodig is om het berichtenvolume te verwerken en de vereiste hogere prestatieniveaus (responstijd) te halen.

Titel 1: de personeelsuitgaven dekken de kosten die verband houden met de aanwerving van extra ICT-personeel om de informatiesystemen van Europol te versterken (zie hierboven). Nadere gegevens over de verdeling van de posten tussen tijdelijke en contractuele functionarissen en hun deskundigheid worden hieronder gegeven.

Titel 3 omvat de kosten voor de hardware en software die nodig zijn om de informatiesystemen van Europol te versterken. Momenteel worden de IT-systemen van Europol door een beperkte, afgebakende groep van Europol-gebruikers, verbindingsofficieren van Europol en onderzoekers in de lidstaten gebruikt voor analyse- en onderzoeksdoeleinden. Na de implementatie van Quest (de systeeminterface waarmee het ESP gegevens van Europol kan doorzoeken) op basisbeschermingsniveau (momenteel zijn de informatiesystemen van Europol geaccrediteerd tot de vertrouwelijkheidsniveaus "EU restricted" en "EU confidential") zal een veel bredere, speciaal daartoe gemachtigde rechtshandhavingsgemeenschap gebruik kunnen maken van de informatiesystemen van Europol. Bovenop deze uitbreidingen komt nog dat het ESP door het ETIAS zal worden gebruikt om de gegevens van Europol automatisch te doorzoeken in het kader van de behandeling van reisautorisaties. Hierdoor zal het aantal opdrachten voor het doorzoeken van Europol-gegevens toenemen van momenteel ongeveer 107 000 per

maand tot meer dan 100 000 per dag, en zullen de informatiesystemen van Europol zeven dagen per week, 24 uur per dag beschikbaar moeten zijn en zeer snel moeten kunnen reageren om aan de vereisten van de ETIAS-verordening te voldoen. Het merendeel van de kosten wordt gemaakt in de periode voordat de interoperabiliteitscomponenten in gebruik worden genomen, maar er zijn ook doorlopende vastleggingen nodig om een grote en constante beschikbaarheid van de informatiesystemen van Europol te garanderen. Bovendien zijn bepaalde ontwikkelingswerkzaamheden nodig voor het implementeren van interoperabiliteitscomponenten door Europol als gebruiker.

18.0205 — Cepol			Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**	Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**TOTAAL**
Titel 1: personeelsuitgaven	Vastleggingen	(1)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
	Betalingen	(2)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
Titel 2: infrastructuur- en operationele uitgaven	Vastleggingen	(1a)	0	0	0	0	0	0	0	0	0	0
	Betalingen	(2a)	0	0	0	0	0	0	0	0	0	0
Titel 3: operationele uitgaven	Vastleggingen	(3a)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
	Betalingen	(3b)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
TOTAAL kredieten voor Cepol	(totaal vastleggingen = totaal betalingen)	=1+1a +3a	0	0,144	0,384	0,482	0,208	0,208	0,208	0,208	0,208	2,050

Centraal gecoördineerde opleiding op EU-niveau zorgt voor meer coherentie in de opleidingscursussen op nationaal niveau en bijgevolg voor een correcte en succesvolle implementatie en benutting van de interoperabiliteitscomponenten. Cepol, het Agentschap van de Europese Unie voor opleiding op het gebied van rechtshandhaving, is goed geplaatst om centrale opleiding op EU-niveau te geven. Deze uitgaven hebben betrekking op de voorbereiding van de "opleidingen voor opleiders uit de lidstaten" op het gebied van het gebruik van de centrale systemen zodra deze zijn interoperabel zijn gemaakt. De kosten omvatten de kosten voor een beperkte personeelsuitbreiding die Cepol in staat moet stellen de cursussen te coördineren, beheren, organiseren en actualiseren, alsook de kosten voor het geven van een aantal opleidingssessies per jaar en voor het organiseren van de onlinecursus. Nadere bijzonderheden over deze kosten worden hieronder toegelicht. De opleidingen worden vooral gegeven in de periode onmiddellijk voorafgaand aan de ingebruikneming. Uit de ervaring met de bestaande opleiding inzake het Schengeninformatiesysteem blijkt dat opleiding ook na de ingebruikneming noodzakelijk blijft, aangezien de interoperabiliteitscomponenten worden onderhouden en er nieuwe opleiders komen.

18.0207 — eu-LISA			Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**	Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**TOTAAL**
Titel 1: personeelsuitgaven	Vastleggingen	(1)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
	Betalingen	(2)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
Titel 2: infrastructuur- en operationele uitgaven	Vastleggingen	(1a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
	Betalingen	(2a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
Titel 3: operationele uitgaven	Vastleggingen	(3a)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
	Betalingen	(3b)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
TOTAAL kredieten voor eu-LISA	(totaal vastleggingen = totaal betalingen)	=1+1a +3a	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**

Deze uitgaven dienen ter dekking van:

– de ontwikkeling en het onderhoud van de vier interoperabiliteitscomponenten (het Europees zoekportaal (ESP), de gezamenlijke dienst voor biometrische matching (gezamenlijke BMS), het gemeenschappelijke identiteitenregister (CIR) en de detector van meerdere identiteiten (MID)) die zijn opgenomen in het wetgevingsvoorstel, plus het centrale register voor rapportage en statistieken (CRRS). eu-LISA zal optreden als vertegenwoordiger van de projecteigenaar en zijn eigen personeel inzetten voor het opstellen van specificaties, het selecteren van contractanten, het aansturen van de werkzaamheden, het indienen van resultaten van een reeks tests en het aanvaarden van het geleverde werk.

– de kosten die gemoeid zijn met de migratie van de gegevens uit de bestaande systemen naar de nieuwe componenten. eu-LISA speelt echter geen rechtstreekse rol bij het opladen van de gegevens voor de MID (het valideren van de links) omdat dit een ingreep is ten aanzien van de inhoud van de gegevens zelf. Bij de migratie van biometrische gegevens uit bestaande systemen spelen alleen het format en de labeling van de gegevens een rol, en niet de inhoud ervan.

– de kosten voor het upgraden en beheren van ECRIS-TCN in hogebeschikbaarheidsmodus vanaf 2022. ECRIS-TCN is het centrale systeem met strafregistergegevens van onderdanen van derde landen. Volgens de planning moet het systeem uiterlijk in 2020 beschikbaar zijn –

eveneens als hogebeschikbaarheidssysteem, aangezien de interoperabiliteitscomponenten er ook toegang toe moeten hebben. De operationele uitgaven omvatten de extra kosten voor het bereiken van die hoge beschikbaarheid. Qua kostenverloop zijn er forse ontwikkelingskosten in 2021, gevolgd door lopende kosten voor onderhoud en beheer. Deze kosten zijn niet opgenomen in het financieel memorandum van de herziening van de verordening tot oprichting van eu-LISA[76], dat alleen de begrotingen van 2018 tot 2020 omvat en dus niet overlapt met dit begrotingsverzoek.

– Het uitgavenpatroon wordt bepaald door de opeenvolging van de onderdelen van het project. Omdat de verschillende componenten niet los staan van elkaar, loopt de ontwikkelingsfase over meerdere jaren, van 2019 tot 2023. Vanaf 2020 gaan de onderhouds- en beheerswerkzaamheden voor de eerste beschikbare componenten echter al van start. Dit verklaart waarom de uitgaven langzaam beginnen, stijgen en dan dalen naar een constante waarde.

– De uitgaven in het kader van titel 1 (personeelsuitgaven) volgen de opeenvolging van de projectonderdelen: voor de oplevering van het project is meer personeel nodig bij de contractant (voor zijn uitgaven: zie titel 3). Na de oplevering wordt een deel van het opleveringsteam ingezet voor evolutie en onderhoud. Tegelijkertijd stijgt het aantal personeelsleden voor het beheer van de pas opgeleverde systemen.

– De uitgaven in het kader van titel 2 (infrastructuur- en operationele uitgaven) dienen ter dekking van de extra kantoorruimte voor de teams van de contractant die tijdelijk worden ingezet voor ontwikkeling, onderhoud en beheer. Het verloop van de uitgaven in de tijd geeft dus ook de evolutie in de personeelsbezetting weer. De kosten voor het hosten van extra apparatuur zijn reeds opgenomen in de begroting van eu-LISA. Er zijn ook geen extra kosten voor het personeel van eu-LISA, aangezien deze zijn opgenomen in de standaard personeelskosten.

– De uitgaven in het kader van titel 3 (operationele uitgaven) omvatten de kosten van de contractant voor de ontwikkeling en het onderhoud van het systeem en de aankoop van specifieke hardware en software.
De initiële kosten van de contractant houden verband met de studies voor het opstellen van de specificaties van de componenten en de ontwikkeling van, in eerste instantie, slechts één component (het CRRS). In de periode 2020-2022 nemen de kosten toe naarmate parallel meer componenten worden ontwikkeld. De kosten nemen na de piek niet af omdat de taken op het gebied van datamigratie bijzonder zwaar zijn bij dit project. De kosten van de contractant dalen naarmate de componenten worden opgeleverd en in gebruik genomen. Hiervoor is qua middelen een stabiel patroon vereist.
Samen met de uitgaven in het kader van titel 3 nemen de uitgaven in 2020 sterk toe ten opzichte van het voorgaande jaar als gevolg van de initiële investeringen in hard- en software tijdens de ontwikkeling. De uitgaven in het kader van titel 3 (operationele uitgaven) stijgen in 2021 en 2022 fors omdat de investeringskosten voor hard- en software voor de operationele IT-omgevingen (productie en preproductie voor zowel de centrale eenheid als de centrale back-upeenheid) worden gemaakt in het jaar vóór de inbedrijfstelling, respectievelijk voor de

[76] Voorstel voor een verordening van het Europees Parlement en de Raad betreffende het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht, tot wijziging van Verordening (EG) nr. 1987/2006 en Besluit 2007/533/JBZ en tot intrekking van Verordening (EU) nr. 1077/2011 (COM 2017/0145 (COD)).

interoperabiliteitscomponenten (het CIR en de MID) met hoge eisen op het gebied van hard- en software. Na de ingebruikneming komen de kosten voor hard- en software hoofdzakelijk neer op onderhoudskosten.

– Voor nadere gegevens: zie verder in de tekst.

Rubriek van het meerjarig financieel kader	**5**	Administratieve uitgaven

miljoen EUR (tot op drie decimalen)

		Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**	Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**TOTAAL**
DG HOME											
• Personele middelen Nummer begrotingsonderdeel 18.01		0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Andere administratieve kosten (vergaderingen, enz.)		0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
TOTAAL DG HOME	Kredieten	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

TOTAAL kredieten voor RUBRIEK 5 van het meerjarig financieel kader	(totaal vastleggingen = totaal betalingen)	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

miljoen EUR (tot op drie decimalen)

		Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**	Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	Jaar **2028**	**TOTAAL**
TOTAAL kredieten voor de RUBRIEKEN 1 tot en met 5	Vastleggingen	**7,533**	**26,569**	**104,672**	**98,591**	**83,363**	**25,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**

van het meerjarig financieel kader	Betalingen	**7,533**	**26,569**	**96,042**	**97,591**	**83,993**	**34,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**

3.2.2. Geraamde gevolgen voor de beleidskredieten

3.2.2.1. Geraamde gevolgen voor de kredieten van het Europees Grens- en kustwachtagentschap

– ☐ Voor het voorstel/initiatief zijn geen beleidskredieten nodig

– ☒ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

Vastleggingskredieten, miljoen EUR (tot op drie decimalen)

Vermeld doelstellingen en outputs **Europees Grens- en kustwachtagentschap** ⇩			Jaar **2019**		Jaar **2020**		Jaar **2021**		Jaar **2022**		Jaar **2023**		Jaar **2024**		Jaar **2025**		Jaar **2026**		Jaar **2027**		**TOTAAL**	
	Soort [77]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 1[78] Validering van links																						
Aantal personeelsleden aangeworven als deskundigen voor het valideren van links	Kosten van de contractant		0	0	0	0	0	0	0,8	0,183	10	2,200	0	0	0	0	0	0	0	0		2,383
Subtotaal specifieke doelstelling nr. 1			**0**	**0**	**0**	**0**	**0**	**0**	**0,8**	**0,183**	**10**	**2,200**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**2,383**

[77] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen, enz.).

[78] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

Deze uitgaven dienen ter dekking van:

- de aanwerving van voldoende extra personeel (naar schatting een tiental deskundigen), naast het bestaande interne personeelsbestand (naar schatting een twintigtal personen), om in het Europees Grens- en kustwachtagentschap links te valideren. Vóór de geplande startdatum is er maar één maand de tijd om het ontbrekende personeel aan te werven.

- Voor het overige zijn er geen contractantkosten geraamd. De benodigde software valt onder de licentiekosten voor de gezamenlijke BMS. Op het gebied van hardware is er geen specifieke verwerkingscapaciteit. Het personeel van de contractant zou worden ondergebracht bij het Europees Grens- en kustwachtagentschap. Daarom zijn in de uitgaven in het kader van titel 2 de jaarlijkse kosten van gemiddeld 12 vierkante meter per persoon toegevoegd.

3.2.2.2. Geraamde gevolgen voor de kredieten van Europol

– ☐ Voor het voorstel/initiatief zijn geen beleidskredieten nodig

– ☒ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

Vastleggingskredieten, miljoen EUR (tot op drie decimalen)

Vermeld doelstellingen en outputs **Europol** ⇩			Jaar **2019**		Jaar **2020**		Jaar **2021**		Jaar **2022**		Jaar **2023**		Jaar **2024**		Jaar **2025**		Jaar **2026**		Jaar **2027**		**TOTAAL**	
	Soort [79]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 1[80] Ontwikkeling en onderhoud van (Europol-)systemen																						
IT-omgeving	Infrastructuur					1,840		1,840		0,736		0,736		0,736		0,736		0,736		0,736		8,096
IT-omgeving	Hardware					3,510		3,510		1,404		1,404		1,404		5,754		5,754		1,404		26,144
IT-omgeving	Software					0,670		0,670		0,268		0,268		0,268		0,268		0,268		0,268		2,948

[79] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen, enz.).

[80] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

Ontwikkeling	Contractant				0,360		0,360												0,720
Subtotaal			**0**		**6,380**		**6,380**		**2,408**		**2,408**		**2,408**		**7,758**		**7,758**		**2,408**		**37,908**

Deze uitgaven dienen om de informatiesystemen en de infrastructuur van Europol te versterken, zodat de toename in het aantal zoekopdrachten kan worden opgevangen. Deze kosten omvatten:

– het upgraden van de beveiligings- en netwerkinfrastructuur, hardware (servers, opslag) en software (licenties). De upgrades moeten plaatsvinden voorafgaand aan de ingebruikneming van het Europees zoekportaal en het ETIAS in 2021. De kosten zijn gelijkelijk verdeeld over 2020 en 2021. Voor de periode vanaf 2022 zijn de onderhoudskosten berekend op basis van een jaarlijks onderhoudsniveau van 20 %. Voorts is uitgegaan van de standaardcyclus van vijf jaar voor het vervangen van verouderde hardware en infrastructuur.

– kosten van de contractant voor ontwikkelingswerkzaamheden met het oog op het implementeren van Quest op basisbeschermingsniveau.

3.2.2.3. Geraamde gevolgen voor de kredieten van Cepol

– ☐ Voor het voorstel/initiatief zijn geen beleidskredieten nodig

– ☒ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

Vastleggingskredieten, miljoen EUR (tot op drie decimalen)

Vermeld doelstellingen en outputs **Cepol** ⇩			Jaar **2019**		Jaar **2020**		Jaar **2021**		Jaar **2022**		Jaar **2023**		Jaar **2024**		Jaar **2025**		Jaar **2026**		Jaar **2027**		**TOTAAL**	
	Soort [81]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 1[82] Ontwikkelen en geven van opleidingen																						
Aantal interne cursussen	0,34 per cursus		0		1	0,040	4	0,136	8	0,272	2	0,068	2	0,068	2	0,068	2	0,068	2	0,068		0,788
Online-opleiding	0,02			0				0,040		0,002		0,002		0,002		0,002		0,002		0,002		0,052
Subtotaal				**0**		**0,040**		**0,176**		**0,274**		**0,070**		**0,070**		**0,070**		**0,070**		**0,070**		**0,840**

[81] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen, enz.).

[82] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

Met het oog op een eenvormige implementatie en benutting van de interoperabiliteitsoplossingen zal de opleiding zowel centraal op EU-niveau door Cepol als door de lidstaten worden georganiseerd. De uitgaven voor opleiding op EU-niveau omvatten:

– de ontwikkeling van een gemeenschappelijk curriculum dat door de lidstaten moet worden gebruikt voor de nationale opleiding;

– interne activiteiten om de opleiders op te leiden. De opleiding zal gedurende de twee jaar onmiddellijk na de ingebruikneming van de interoperabiliteitsoplossingen waarschijnlijk op grotere schaal plaatsvinden en vervolgens op peil worden gehouden met twee interne cursussen per jaar.

– online-cursus ter aanvulling van de interne activiteiten op EU-niveau en in de lidstaten.

3.2.2.4. Geraamde gevolgen voor de kredieten van eu-LISA

– ☐ Voor het voorstel/initiatief zijn geen beleidskredieten nodig

– ☒ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

Vastleggingskredieten, miljoen EUR (tot op drie decimalen)

Vermeld doelstellingen en outputs eu-LISA ⇩			Jaar **2019**		Jaar **2020**		Jaar **2021**		Jaar **2022**		Jaar **2023**		Jaar **2024**		Jaar **2025**		Jaar **2026**		Jaar **2027**		**TOTAAL**	
	Soort [83]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 1[84] Ontwikkeling van de interoperabiliteitscomponenten																						
Gebouwde systemen	Contractant			1,800		4,930		8,324		4,340		1,073		1,000		0,100		0,020		0,020		21,607
Softwareproducten	Software			0,320		3,868		15,029		8,857		3,068		0,265		0,265		0,265		0,265		32,202
Hardwareproducten	Hardware			0,250		2,324		5,496		2,904		2,660		0,500		0		0		0		14,133
IT-opleiding	Opleiding & andere			0,020		0,030		0,030		0,030		0,030		0,050		0,050		0,050		0,050		0,340

[83] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen, enz.).

[84] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

Subtotaal specifieke doelstelling nr. 1		**2,390**		**11,151**		**28,879**		**16,131**		**6,830**		**1,815**		**0,415**		**0,335**		**0,335**		**68,281**

– Deze doelstelling omvat alleen de kosten voor de oplevering van de vier interoperabiliteitscomponenten en het CRRS.

– Bij de raming van de kosten voor de gezamenlijke BMS is ervan uitgegaan dat het EES, dat spoedig zal worden ontwikkeld, dienst zal doen als spilsysteem voor de ontwikkeling. Daarom is het de bedoeling de biometrische softwarelicenties (36 miljoen EUR) voor het EES te hergebruiken.

– In deze begroting wordt de gezamenlijke BMS vanuit budgettair oogpunt behandeld als een verdere uitbreiding van de BMS voor het EES. Daarom zijn in dit financieel memorandum de marginale kosten opgenomen voor softwarelicenties (6,8 miljoen EUR) om ongeveer 20 miljoen biometrische datareeksen uit het AFIS van het SIS (AFIS is het geautomatiseerd systeem voor de identificatie van vingerafdrukken, oftewel de "BMS van het SIS"), het AFIS van Eurodac en het toekomstige ECRIS-TCN (Europees Strafregister Informatiesysteem voor onderdanen van derde landen) toe te voegen aan de BMS die wordt geleverd voor het EES. De kosten voor de integratie van de verschillende systemen (SIS, Eurodac, ECRIS-TCN) in de gezamenlijke BMS zijn in dit financieel memorandum opgenomen.

– Als onderdeel van de werkzaamheden in 2019 en 2020 zal aan eu-LISA worden gevraagd om de juiste technische oplossing uit te werken (deze kan bij het indienen van het wetsvoorstel nog niet nader worden omschreven) en om te ramen welke gevolgen de uitvoering van de gekozen technische oplossing zal hebben voor de kosten. Het is mogelijk dat de hier opgevoerde kostenraming dan dienovereenkomstig moet worden aangepast.

– Eind 2023 moeten alle componenten geleverd zijn. Dit verklaart waarom de uitgaven van de contractant tegen die tijd tot nagenoeg nul teruglopen. Het enige bedrag dat overblijft, is dat voor het periodiek updaten van het CRRS.

– In de periode 2019-2021 stijgen de uitgaven voor software sterk onder invloed van de softwarelicentiekosten voor de verschillende omgevingen die nodig zijn voor de productie-, preproductie- en testfase, zowel op de centrale locatie als op de back-uplocatie. Bovendien hangt de prijs van een aantal specifieke en onmisbare softwarecomponenten samen met het aantal "gerefereerde objecten" (dat wil zeggen het datavolume). Aangezien de databank uiteindelijk ca. 220 miljoen identiteiten zal bevatten, is de prijs van de software evenredig aan deze waarde.

Vermeld doelstellingen en outputs eu-LISA ⇩			Jaar 2019		Jaar 2020		Jaar 2021		Jaar 2022		Jaar 2023		Jaar 2024		Jaar 2025		Jaar 2026		Jaar 2027		TOTAAL	
	Soort 85	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 2 Onderhoud en beheer van de interoperabiliteitscomponenten																						
Operationeel gehouden systemen	Contractant			0		0		0		1,430		2,919		2,788		2,788		2,788		2,788		15,501
Softwareproducten	Software			0		0,265		0,265		1,541		5,344		5,904		5,904		5,904		5,904		31,032
Hardwareproducten	Hardware			0		0,060		0,060		0,596		1,741		1,741		1,741		1,741		1,741		9,423
IT-opleiding	Opleiding			0		0		0		0		0,030		0,030		0,030		0,030		0,030		0,150
Subtotaal specifieke doelstelling nr. 2				**0**		**0,325**		**0,325**		**3,567**		**10,034**		**10,464**		**10,464**		**10,464**		**10,464**		**56,105**

– Het onderhoud begint zodra een aantal componenten wordt geleverd. Daarom is vanaf de oplevering van het ESP (in 2021) voorzien in een budget voor een onderhoudscontractant. De begroting voor onderhoud neemt toe naarmate meer componenten worden opgeleverd en blijft dan min of meer stabiel, op een niveau van 15 tot 22 % van de initiële investering.

[85] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen, enz.).

– Het onderhoud van de hardware en software begint vanaf het jaar van ingebruikneming: het kostenverloop is vergelijkbaar met dat voor de contractant.

Vermeld doelstellingen en outputs **eu-LISA** ⇩			Jaar **2019**		Jaar **2020**		Jaar **2021**		Jaar **2022**		Jaar **2023**		Jaar **2024**		Jaar **2025**		Jaar **2026**		Jaar **2027**		**TOTAAL**	
	Soort [86]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 3[87] Datamigratie																						
Migratie van bestaande BMS-	naar de gezamenlijke			0		0		0		7,000		3,000		0		0		0		0		10,000
Migratieklaar maken van bestaande EDAC-gegevens	Wijzigen van het ontwerp en de architectuur van EDAC			0		0		7,500		7,500				0		0		0		0		15,000
Subtotaal specifieke doelstelling nr. 3				**0**		**0**		**7,500**		**14,500**		**3,000**										**25,000**

– De migratie van data van de andere biometrische zoekmachines naar de gezamenlijke BMS is noodzakelijk omdat dit gemeenschappelijke systeem operationeel doeltreffender is en financieel voordeliger dan het behoud van meerdere kleinere BMS-systemen.

– In tegenstelling tot bij het VIS is het mechanisme voor het matchen van biometrische gegevens bij Eurodac niet duidelijk afgescheiden. De interne werking van Eurodac en het mechanisme waarmee de zakelijke diensten de onderliggende diensten voor de biometrische matching

[86] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen, enz.).

[87] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

oproepen is een zwarte doos voor de buitenstaander en is gebaseerd op eigendomstechnologie. Het zal niet mogelijk zijn om de data gewoonweg naar een gezamenlijke BMS te migreren en de bestaande zakelijke laag te behouden. De datamigratie zal daarom gepaard gaan met aanzienlijke kosten voor het wijzigen van de mechanismen voor de uitwisseling met de centrale Eurodac-applicatie.

Vermeld doelstellingen en outputs **eu-LISA** ⇩			Jaar **2019**		Jaar **2020**		Jaar **2021**		Jaar **2022**		Jaar **2023**		Jaar **2024**		Jaar **2025**		Jaar **2026**		Jaar **2027**		**TOTAAL**	
	Soort [88]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 4[89] Netwerk																						
Netwerkverbindingen	Opzetten van het netwerk			0		0		0		0,505										0		0,505
Verwerkt netwerkverkeer	Netwerkbeheer			0		0						0,246		0,246		0,246		0,246		0,246		1,230
Subtotaal specifieke doelstelling nr. 4				**0**		**0**		**0**		**0,505**		**0,246**		**0,246**		**0,246**		**0,246**		**0,246**		**1,735**

– De interoperabiliteitscomponenten hebben slechts een marginaal effect op het netwerkverkeer. Omdat er slechts links tussen bestaande gegevens worden gecreëerd, blijft het datavolume laag. Hier zijn enkel de marginaal toenemende kosten opgenomen die nodig zijn bovenop het budget van het EES en het ETIAS voor het opzetten van het netwerk en het netwerkverkeer.

[88] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen, enz.).

[89] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

Vermeld doelstellingen en outputs eu-LISA ⇩			Jaar **2019**		Jaar **2020**		Jaar **2021**		Jaar **2022**		Jaar **2023**		Jaar **2024**		Jaar **2025**		Jaar **2026**		Jaar **2027**		**TOTAAL**	
	Soort [90]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 5[91] Update NUI																						
Geüpdatete NUI	Contractant			0		0		0		0,505		0,505								0		1,010
Subtotaal specifieke doelstelling nr. 5				**0**		**0**		**0**		**0,505**		**0,505**										**1,010**

– Het concept van de uniforme nationale interface (NUI) die moet worden ontwikkeld en onderhouden door eu-LISA, is afkomstig uit het EES-voorstel. De bovenstaande tabel bevat de begroting om de NUI te updaten voor een extra soort informatie-uitwisseling. De beheerskosten voor de NUI, die al opgenomen waren in het begrotingsvoorstel voor het EES, zullen niet toenemen.

[90] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen, enz.).

[91] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

Vermeld doelstellingen en outputs eu-LISA ⇩			Jaar 2019		Jaar 2020		Jaar 2021		Jaar 2022		Jaar 2023		Jaar 2024		Jaar 2025		Jaar 2026		Jaar 2027		TOTAAL	
	Soort[92]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 6 Vergaderingen en opleiding																						
Maandelijkse follow-upvergaderingen (Ontwikkeling)	0,021 per vergadering × 10 per jaar		10	*0,210*	10	*0,210*	10	*0,210*	10	*0,210*											40	0,840
Driemaandelijkse vergaderingen (beheer)	0,021 × 4 per jaar		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Adviesgroepen	0,021 × 4 per jaar		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Opleiding lidstaten	0,025 per opleiding		2	0,050	4	0,100	4	0,100	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	24	1,150
Subtotaal specifieke			20	**0,428**	22	**0,478**	22	**0,478**	24	**0,528**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**		**3,502**

[92] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen, enz.).

doelstelling nr. 6																		

– Het subtotaal omvat de kosten van de vergaderingen die door de beheersautoriteit (in dit geval eu-LISA) worden georganiseerd om het project te beheren. Dit zijn de kosten voor extra vergaderingen voor de oplevering van de interoperabiliteitscomponenten.

– Het subtotaal omvat de kosten voor vergaderingen van eu-LISA met personeelsleden van de lidstaten die zich bezighouden met de ontwikkeling, het onderhoud en het beheer van de interoperabiliteitscomponenten en met het organiseren en geven van opleiding aan het IT-personeel van de lidstaten.

– Tijdens de ontwikkeling voorziet de begroting in tien projectvergaderingen per jaar. Tijdens de voorbereiding (met ingang van 2019) van de ingebruikneming worden dat er vier per jaar. Op een hoger niveau wordt meteen in het begin een adviesgroep opgericht om de uitvoeringsbesluiten van de Commissie uit te voeren. Deze groep komt, net als de bestaande adviesgroepen, vier keer per jaar bijeen. eu-LISA zorgt voor het voorbereiden en geven van opleiding aan het IT-personeel in de lidstaten. De opleiding betreft de technische aspecten van de interoperabiliteitscomponenten.

Vermeld doelstellingen en outputs eu-LISA ⇩			Jaar 2019		Jaar 2020		Jaar 2021		Jaar 2022		Jaar 2023		Jaar 2024		Jaar 2025		Jaar 2026		Jaar 2027		TOTAAL	
	Soort [93]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 7[94] Hoge beschikbaarheid ECRIS-TCN																						
Systeem met hoge beschikbaarheid	Opzetten van het systeem			0		0		8,067												0		8,067
Beheer van de hoge beschikbaarheid	Onderhoud en beheer van het systeem			0		0		0		1,768		1,768		1,768		1,768		1,768		1,768		10,608
Subtotaal specifieke doelstelling nr. 7				**0**		**0**		**8,067**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**18,675**

– De doelstelling bestaat erin om van het ECRIS-TCN een systeem met een hoge – in plaats van een "standaard" – beschikbaarheid te maken. Daarvoor is met name een upgrade met extra hardware nodig, die in 2021 zou worden geïnstalleerd. Aangezien het ECRIS-TCN in 2020 klaar moet zijn, is het aanlokkelijk om dat systeem van meet af aan te bouwen als een hogebeschikbaarheidssysteem dat geïntegreerd is met de interoperabiliteitscomponenten. Gezien de onderlinge verwevenheid van een groot aantal projecten is het echter raadzaam af te stappen van dat scenario en afzonderlijke acties in de begroting te voorzien. Dit is een aanvullende begroting voor de kosten van de ontwikkeling, het onderhoud en het beheer van het ECRIS-TCN) in 2019 en 2020.

[93] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen, enz.).

[94] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

3.2.2.5. Geraamde gevolgen voor de kredieten van DG HOME

– ☐ Voor het voorstel/initiatief zijn geen beleidskredieten nodig

– ☒ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

Vastleggingskredieten, miljoen EUR (tot op drie decimalen)

Vermeld doelstellingen en outputs **DG HOME** ⇩			Jaar **2019**		Jaar **2020**		Jaar **2021**		Jaar **2022**		Jaar **2023**		Jaar **2024**		Jaar **2025**		Jaar **2026**		Jaar **2027**		**TOTAAL**	
	Soort [95]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 1 Integratie van nationale systemen (van de lidstaten)																						
Gebruiksklare NUI	Aanpassing van de NUI – ontwikkeling						30	3,150	30	3,150											30	6,300
Voor interoperabiliteit aangepaste systemen van de lidstaten	Integratiekosten						30	40,000	30	40,000	30	40,000									30	120,000

[95] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen, enz.).

Eindgebruikers opgeleid	10 000 eindgebruikersessies; in totaal 1 000 EUR per							5000	5,000	5000	5,000									10.000	10,000
Subtotaal specifieke doelstelling nr. 1							**43,150**		**48,150**		**45,000**										**136,300**

– Deze specifieke doelstelling heeft betrekking op de financiële middelen die ter beschikking van de lidstaten worden gesteld zodat zij de vruchten van interoperabele centrale systemen kunnen plukken. De NUI wordt aangepast bij de implementatie van het ESP en de ingebruikneming van de MID. Vervolgens moet elke lidstaat een relatief bescheiden aanpassing (geraamd op 150 mandagen) uitvoeren zodat het geüpdatete berichtenverkeer met de centrale systemen kan plaatsvinden. Substantiëler is de wijziging van de inhoud van de gegevens als gevolg van de interoperabiliteit. De hiermee verbonden kosten vallen onder de "integratiekosten". Deze middelen dienen ter dekking van veranderingen in het type berichten die naar aan het centrale systeem worden gestuurd en de verwerking van het antwoord op deze berichten. Om deze wijzigingen te bekostigen, is een budget van 4 miljoen EUR per lidstaat toegewezen. Dit bedrag is hetzelfde als voor het EES aangezien de werklast om de integratie van de nationale systemen en de NUI aan te passen, vergelijkbaar is.

– De eindgebruikers moeten worden opgeleid. Deze opleiding voor een zeer grote groep eindgebruikers wordt gefinancierd op basis van een bedrag van 1 000 EUR per sessie van 10 tot 20 eindgebruikers voor naar schatting 10 000 sessies die door de lidstaten in hun eigen bedrijfsruimten worden georganiseerd.

3.2.3. Geraamde gevolgen voor personele middelen

3.2.3.1. Samenvatting – Europees Grens- en kustwachtagentschap

☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

☒ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

miljoen EUR (tot op drie decimalen)

	Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**	Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**TOTAAL**
Ambtenaren (AD)										
Ambtenaren (AST)	0									
Arbeidscontractanten	0	0	0	0,350	1,400	0,233	0	0	0	1,983
Tijdelijke functionarissen	0	0	0	0	0	0	0	0	0	0
Gedetacheerde nationale deskundigen										
TOTAAL	**0,0**	**0,0**	**0,0**	**0,350**	**1,400**	**0,233**	**0,0**	**0,0**	**0,0**	**1,983**

Het werk dat het aan het Europees Grens- en kustwachtagentschap toegevoegde personeel op dit gebied zal moeten uitvoeren, is tijdelijk (2023) en gaat van start 24 maanden nadat de biometrische zoekmachine voor het EES beschikbaar komt. Het personeel moet echter vooraf (gemiddeld drie maanden eerder) worden aangeworven – vandaar het cijfer voor 2022. Na het eigenlijke werk worden twee maanden uitgetrokken om alles af te ronden – dit verklaart het personeelsniveau in 2024.

Wat het voor het vereiste werk benodigde personeel zelf betreft, wordt uitgegaan van twintig personen (plus de inzet van 10 personen door een contractant – zie titel 3). Verwacht wordt dat het werk niet binnen de normale kantooruren kan worden uitgevoerd en langere werktijden zal vergen. Het agentschap wordt verondersteld voor ondersteunend en leidinggevend personeel te zorgen.

Het aantal personeelsleden is gebaseerd op de veronderstelling dat ongeveer 550 000 vingerafdrukken moeten worden beoordeeld en elk geval gemiddeld 5 tot 10 minuten in beslag neemt (17 000 afdrukken per jaar gecontroleerd)[96].

[96] Gegevens over het personeel in 2020 en later zijn indicatief. Beoordeeld moet worden of dit personeel al dan niet wordt toegevoegd aan de personeelsramingen voor het Europees Grens- en kustwachtagentschap (zoals opgenomen in COM(2015) 671)

Aantal personeelsleden	2019	2020	2021	2022	2023	2024	2025	2026	2027	Totaal
Personeel voor manuele verwerking van links en besluiten	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Totaal Titel 1 - Arbeidscontractanten	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Totaal Titel 1 - Tijdelijke functionarissen	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Totaal Titel 1	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3

.

3.2.3.2. Samenvatting – Europol

☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

☒ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

miljoen EUR (tot op drie decimalen)

	Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**	Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**TOTAAL**
Ambtenaren (AD)										
Ambtenaren (AST)	0									
Arbeidscontractanten	0,000	0,070	0,070	0,560	0,560	0,560	0,560	0,560	0,560	3,500
Tijdelijke functionarissen	0,690	1,932	1,932	0,621	0,621	0,414	0,414	0,414	0,414	7,452
Gedetacheerde nationale deskundigen										
TOTAAL	**0,690**	**2,002**	**2,002**	**1,181**	**1,181**	**0,974**	**0,974**	**0,974**	**0,974**	**10,952**

Deze kosten worden geraamd op basis van de volgende personeelsbezetting:

Aantal VTE voor ICT	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Totaal**
Arbeidscontractanten	0,0	1,0	1,0	8,0	8,0	8,0	8,0	8,0	8,0	50,0
Tijdelijke functionarissen	5,0	14,0	14,0	4,5	4,5	3,0	3,0	3,0	3,0	54,0
Totaal personeel (VTE)	**5,0**	**15,0**	**15,0**	**12,5**	**12,5**	**11,0**	**11,0**	**11,0**	**11,0**	**104,0**

De inzet van extra ICT-personeel voor Europol wordt overwogen, om de informatiesystemen van Europol te versterken, de toename van het aantal zoekopdrachten van het ESP en het ETIAS te verwerken en de systemen vervolgens 24/7 (zeven dagen per week, 24 uur per dag) operationeel te houden.

– Voor de implementatie van het ESP (in 2020 en 2021) zijn meer technisch deskundigen nodig (architecten, ingenieurs, ontwikkelaars, testers). Voor de periode vanaf 2022 zal een kleiner aantal technisch deskundigen volstaan om de rest van de interoperabiliteitscomponenten te implementeren en de systemen te onderhouden.

– Vanaf de tweede helft van 2021 moet het ICT-systeem 24/7 worden gemonitord om het niveau van dienstverlening van het ESP en het ETIAS te garanderen. Dit werk zal in vierploegendienst worden verricht door twee arbeidscontractanten, 24/7.

– De profielen zijn zo goed mogelijk verdeeld over tijdelijke functionarissen en arbeidscontractanten. Er zij op gewezen dat vanwege de hoge veiligheidseisen, op sommige posten alleen tijdelijke functionarissen worden ingezet. Bij het verzoek om tijdelijke functionarissen zal rekening worden gehouden met de resultaten van de bemiddeling over de begrotingsprocedure 2018.

3.2.3.3. Samenvatting – Cepol

☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

☒ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

miljoen EUR (tot op drie decimalen)

	Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**	Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**TOTAAL**
Ambtenaren (AD)										
Ambtenaren (AST)										
Arbeidscontractanten			0,070	0,070						**0,140**
Tijdelijke functionarissen		0,104	0,138	0,138	0,138	0,138	0,138	0,138	0,138	1,070
Gedetacheerde nationale deskundigen										
TOTAAL		**0,104**	**0,208**	**0,208**	**0,138**	**0,138**	**0,138**	**0,138**	**0,138**	**1,210**

Er is extra personeel nodig omdat de opleiding voor de opleiders van de lidstaten specifiek moet worden ontwikkeld met het oog op het gebruik van de interoperabiliteitscomponenten in operationele omstandigheden.

- Uiterlijk acht maanden voordat het systeem in gebruik wordt genomen, moet met de ontwikkeling van het curriculum en opleidingsmodules worden begonnen. Tijdens de eerste twee jaar na de ingebruikneming is de opleiding het intensiefst. Voor een coherente implementatie is het echter van belang het opleidingsniveau gedurende een langere periode op peil te houden, zoals blijkt uit de ervaringen met het Schengeninformatiesysteem.

- Het extra personeel is nodig voor de voorbereiding, coördinatie en uitvoering van het curriculum, de interne cursussen en de online-cursus. Deze cursussen komen bovenop de bestaande opleidingscatalogus van Cepol en vereisen bijgevolg extra personeel.

- Tijdens de volledige ontwikkelings- en onderhoudsperiode zou een tijdelijke functionaris het cursusbeheer op zich nemen, met ondersteuning van een arbeidscontractant tijdens de drukste organisatieperiode.

3.2.3.4. Samenvatting – eu-LISA

☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

☒ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

miljoen EUR (tot op drie decimalen)

	Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**	Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**TOTAAL**
Ambtenaren (AD)										
Ambtenaren (AST)										
Arbeidscontractanten	0,875	1,400	1,855	2,555	2,415	2,170	2,100	2,100	2,100	17,570
Tijdelijke functionarissen	2,001	3,450	4,347	4,347	4,209	3,312	3,036	3,036	3,036	30,774
Gedetacheerde nationale deskundigen										
TOTAAL	**2,876**	**4,850**	**6,202**	**6,902**	**6,624**	**5,482**	**5,136**	**5,136**	**5,136**	**48,344**

– Bij het bepalen van de personeelsvereisten is er rekening mee gehouden dat de componenten en het CRRS een geheel van met elkaar samenhangende projecten vormen (d.w.z. een programma). Om de samenhang tussen de projecten te beheren, wordt een programmabeheerteam opgericht, bestaande uit de programma- en projectbeheerders en de personen met een bepaald profiel die moeten omschrijven wat zij gemeen hebben. Om het programma/project te realiseren, zijn ook ondersteunende profielen nodig.

– De raming van de personeelsbehoeften per project is geënt op die voor eerdere projecten (het Visuminformatiesysteem) en is opgesplitst in twee delen: voltooiing van het project en operationele fase.

– Voor profielen die tijdens de operationele fase vereist zijn, worden tijdelijke functionarissen aangeworven. Voor profielen die nodig zijn tijdens de uitvoering van het programma/project, worden arbeidscontractanten aangeworven. Om de verwachte continuïteit van de taakuitvoering te waarborgen en om kennis binnen het agentschap te houden, wordt het aantal posten bijna gelijkelijk verdeeld over tijdelijke functionarissen en arbeidscontractanten.

– Waarschijnlijk zal geen extra personeel nodig zijn voor het project om van het ECRIS-TCN een hogebeschikbaarheidssysteem te maken, en zal voor het eu-LISA-project bestaand personeel van projecten worden gehaald die in die periode op hun einde lopen.

Deze ramingen zijn gebaseerd op de volgende personeelsbezetting:

Voor arbeidscontractanten:

3.2.1. outputs eu-LISA (gelijk aan T1) in aantal personen	2019	2020	2021	2022	2023	2024	2025	2026	2027	Totaal (formule)
Arbeidscontractanten										-
Programma-/projectbeheer	4,0	5,0	5,5	5,5	4,5	3,0	3,0	3,0	3,0	36,5
CRRS PB	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*1,5*
MID	*0,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*2,0*
Programma-/projectkantoor	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*14,0*
Kwaliteitsborging	*1,0*	*2,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*19,0*
Financiën en aankoop	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Financieel beheer										*0,0*
Budgettaire planning en controle										*0,0*
Aankoop-/contractbeheer	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Technisch deskundigen	7,0	7,0	7,0	7,0	6,0	5,0	5,0	5,0	5,0	54,0
CRRS	*3,0*	*3,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*22,0*
ESP	*4,0*	*4,0*	*4,0*	*4,0*	*4,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Gezamenlijke BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Tests	1,5	3,0	4,0	4,0	4,0	3,0	2,0	2,0	2,0	25,5
CRRS	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*6,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Gezamenlijke BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,5*	*1,0*	*2,0*	*2,5*	*2,5*	*1,5*	*1,0*	*1,0*	*1,0*	*13,0*
MID	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*6,5*
Systeemmonitoring	0,0	5,0	10,0	20,0	20,0	20,0	20,0	20,0	20,0	135,0
Gemeenschappelijk (24:7)	0,0	*5,0*	*10,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*135,0*
Algemene coördinatie	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Personele middelen	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
HR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Subtotaal Arbeidscontractanten	**12,5**	**20,0**	**26,5**	**36,5**	**34,5**	**31,0**	**30,0**	**30,0**	**30,0**	**251,0**

Voor tijdelijke functionarissen:

Tijdelijke functionarissen										
Programma-/projectbeheer	3,0	4,0	5,5	5,5	5,5	4,5	4,0	4,0	4,0	40,0
Programmabeheerder	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Projectbeheer	*0,0*	*0,0*	*1,0*	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*12,0*
Programma-/projectkantoor	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
ESP	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
Gezamenlijke BMS	*0,5*	*0,5*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*4,0*
CIR	*0,0*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Financiën en aankoop	3,0	3,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	34,0
Financieel beheer	*0,0*	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*7,0*
Budgettaire planning en controle	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Aankoop-/contractbeheer	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*18,0*
Technisch deskundigen	6,0	14,0	17,0	17,0	15,0	11,0	10,0	10,0	10,0	110,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Gezamenlijke BMS	*2,0*	*3,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
CIR	*2,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Beveiliging	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*17,0*
MID	*0,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*12,0*
Architecten	*1,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,0*	*1,0*	*1,0*	*17,0*
Tests	2,5	3,0	4,0	4,0	4,0	2,5	2,0	2,0	2,0	26,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,5*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*6,5*
Gezamenlijke BMS	*2,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,5*	*1,5*	*1,5*	*19,5*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Systeemmonitoring	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Gezamenlijke BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Opleiding	0,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	8,0
Opleiding	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*8,0*
Personele middelen	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Personele middelen	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Andere	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	5,0
Expert gegevensbescherming	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	*5,0*
Subtotaal Tijdelijke functionarissen	**14,5**	**25,0**	**31,5**	**31,5**	**30,5**	**24,0**	**22,0**	**22,0**	**22,0**	**223,0**
Totaal	**27,0**	**45,0**	**58,0**	**68,0**	**65,0**	**55,0**	**52,0**	**52,0**	**52,0**	**474,0**

3.2.4. Geraamde gevolgen voor de administratieve kredieten

3.2.4.1. Samenvatting – DG Home

– ☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

– ☒ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

miljoen EUR (tot op drie decimalen)

	Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**	Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**TOTAAL**
RUBRIEK 5 van het meerjarig financieel kader										
Personele middelen DG HOME	0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Andere administratieve uitgaven	0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
Subtotaal RUBRIEK 5 van het meerjarig financieel kader	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Buiten RUBRIEK 5[97] van het meerjarig financieel kader	(Niet gebruikt)									
Personele middelen										
Andere administratieve uitgaven										
Subtotaal buiten RUBRIEK 5 van het meerjarig financieel kader										

TOTAAL	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

.

97 Technische en/of administratieve bijstand en uitgaven ter ondersteuning van de uitvoering van programma's en/of acties van de EU (vroegere "BA"-onderdelen), onderzoek door derden, eigen onderzoek.

3.2.4.2. Geraamde personeelsbehoeften

– ☐ Voor het voorstel/initiatief zijn geen personele middelen nodig.

– ☒ Voor het voorstel/initiatief zijn personele middelen nodig, zoals hieronder nader wordt beschreven:

Raming in voltijdequivalenten

	Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**	Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**TOTAAL**
• Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)										
18 01 01 01 (zetel en vertegenwoordigingen van de Commissie) DG HOME	5,0	5,0	5,0	5,0	5,0	5,0	2,0	2,0	2,0	36,0
XX 01 01 02 (delegaties)										
XX 01 05 01 (onderzoek door derden)										
10 01 05 01 (eigen onderzoek)										
• Extern personeel (in voltijdequivalenten VTE)[98]										
XX 01 02 02 (AC, AL, END, INT en JED in de delegaties)										
XX 01 04 **JJ** [99] - zetel										
XX 01 04 **JJ** [99] - delegaties										
XX 01 05 02 (AC, END, INT - onderzoek door derden)										
10 01 05 02 (AC, END, INT - eigen onderzoek)										
Ander begrotingsonderdeel (geef aan welk)										
TOTAAL	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**2,0**	**2,0**	**2,0**	**36,0**

18 is het beleidsterrein of de begrotingstitel.

De benodigde personele middelen zullen worden gefinancierd uit de middelen die reeds voor het beheer van deze actie zijn toegewezen en/of binnen het DG zijn herverdeeld, eventueel aangevuld met middelen die in het kader van de jaarlijkse toewijzingsprocedure met inachtneming van de budgettaire beperkingen aan het beherende DG kunnen worden toegewezen.

Beschrijving van de uit te voeren taken

Monitoring en follow-up van het project. Drie ambtenaren voor de follow-up. Bij de uitvoering van het programma vervult het personeel de taken van de Commissie: het controleert de naleving van het wetgevingsvoorstel en pakt problemen op dit gebied aan, stelt verslagen op voor het Europees Parlement en de Raad, en beoordeelt de vooruitgang van de lidstaten. Aangezien de taken in verband met het programma bovenop de gewone werklast komen, is extra personeel nodig. Het personeelsbestand neemt slechts tijdelijk toe, en enkel in de ontwikkelingsperiode.

Beheer van de UMF-norm (Universal Message Format)

De Commissie zorgt voor het dagelijkse beheer van de UMF-norm. Hiervoor zijn twee ambtenaren nodig: een deskundige op het gebied van rechtshandhaving en een andere persoon met een grondige kennis op het vlak van bedrijfsmodellering en ICT.

[98] AC= agent contractuel (arbeidscontractant); AL = agent local (plaatselijk functionaris); AL = agent local (plaatselijk functionaris);END = expert national détaché (gedetacheerd nationaal deskundige); INT = intérimaire (uitzendkracht); JED= jeune expert en délégation (jonge deskundige in delegaties).

[99] Subplafond voor extern personeel uit beleidskredieten (vroegere "BA"-onderdelen).

Deze norm heeft betrekking op gestructureerde, grensoverschrijdende informatie-uitwisseling tussen informatiesystemen, autoriteiten en/of organisaties op het gebied van justitie en binnenlandse zaken. In de UMF-norm worden een gemeenschappelijk vocabularium en logische structuren voor informatie-uitwisseling vastgesteld met als doel de interoperabiliteit te bevorderen door het mogelijk te maken de inhoud van de uitwisseling op een consistente en semantisch gelijkwaardige manier te creëren en te lezen.

Om eenvormige voorwaarden voor de toepassing van het UMF te waarborgen, wordt voorgesteld om uitvoeringsbevoegdheden aan de Commissie toe te kennen. Volgens het voorstel moeten deze bevoegdheden worden uitgeoefend overeenkomstig Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren.

3.2.5. Verenigbaarheid met het huidig meerjarig financieel kader

– ☐ Het voorstel/initiatief is verenigbaar met het huidig meerjarig financieel kader.

– ☒ Het voorstel/initiatief vergt herprogrammering van de betrokken rubriek van het meerjarig financieel kader.

Zet uiteen welke herprogrammering nodig is, onder vermelding van de betrokken begrotingsonderdelen en de desbetreffende bedragen. De ISF-grenzenverordening is het financiële instrument waarin het budget voor de uitvoering van het interoperabiliteitsinitiatief is opgenomen. In artikel 5, lid 5, onder b), is daarom voorzien in een bedrag van 791 miljoen EUR voor de ontwikkeling van IT-systemen gebaseerd op bestaande en/of nieuwe IT-systemen ter beheersing van de migratiestromen langs de buitengrenzen, onder voorbehoud van de vaststelling van de desbetreffende wetgevingshandelingen van de Unie, en onder de voorwaarden van artikel 15. Van deze 791 miljoen EUR is 480,2 miljoen EUR gereserveerd voor de ontwikkeling van het EES, 210 miljoen EUR voor het ETIAS en 67,9 miljoen EUR voor de herziening van het SIS II. De rest (32,9 miljoen EUR) dient te worden herschikt via de ISF-B-mechanismen. **Binnen de looptijd van het huidige MFK is voor het onderhavige voorstel een bedrag 32,1 miljoen EUR nodig – wat past in het resterende budget.**

De conclusie in het vak hierboven over het vereiste bedrag van 32,1 miljoen EUR is het resultaat van de volgende berekening:

VASTLEGGINGEN										
3.2. Geraamde gevolgen voor de uitgaven DG HOME										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Totaal (horiz.)**
18 02 01 03 - Slimme grenzen (incl. steun voor LS)	0	0	43,150	48,150	45,000	0	0	0	0	136,300
Totaal (1)	**0**	**0**	**43,150**	**48,150**	**45,000**	**0**	**0**	**0**	**0**	**136,300**
18.0207 -3.2. eu-LISA										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Totaal (formule)**
T1: personeelsuitgaven	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
T2: infrastructuur- en operationele uitgaven	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
T3: operationele uitgaven	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
Totaal (2)	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**
		22,861							**202,181**	**225,041**
18.02.04 -3.2. Europol										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Totaal (formule)**
T1: personeelsuitgaven	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
T2: infrastructuur- en operationele uitgaven	0	0	0	0	0	0	0	0	0	0
T3: operationele uitgaven	0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
Totaal (3)	**0,690**	**8,382**	**8,382**	**3,589**	**3,589**	**3,382**	**8,732**	**8,732**	**3,382**	**48,860**
		9,072							39,788	48,860
18.02.05 -3.2. Cepol										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Totaal (formule)**
T1: personeelsuitgaven	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
T2: infrastructuur- en operationele uitgaven	0	0	0	0	0	0	0	0	0	0
T3: operationele uitgaven	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
Totaal (4)	**0**	**0,144**	**0,384**	**0,482**	**0,208**	**0,208**	**0,208**	**0,208**	**0,208**	**2,050**
		0,144							**1,906**	**2,050**
18.02.0 -3.2. Frontex - EGKW										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Totaal (formule)**
T1: personeelsuitgaven	0	0	0	0,350	1,400	0,233	0	0	0	1,983
T2: infrastructuur- en operationele uitgaven	0	0	0	0,075	0,300	0,050	0	0	0	0,425
T3: operationele uitgaven	0	0	0	0,183	2,200	0	0	0	0	2,383
Totaal (5)	**0**	**0**	**0**	**0,608**	**3,900**	**0,283**	**0**	**0**	**0**	**4,792**
		0							**4,792**	**4,792**
TOTAAL (1)+(2)+(3) +(4) +(5)	6,520	25,556	103,659	97,578	82,350	24,243	27,549	27,469	22,119	417,043
		32,076							384,966	
3.2. DG HOME Rubriek 5 'Administratieve uitgaven'										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Totaal**
Totaal (6)	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695
TOTAAL (1)+(2)+(3)+(4)+(5)+(6)	7,533	26,569	104,672	98,591	83,363	25,256	28,088	28,008	22,658	424,738

– ☐ Het voorstel/initiatief vergt toepassing van het flexibiliteitsinstrument of herziening van het meerjarige financiële kader.

3.2.6. Bijdragen van derden

– Het voorstel/initiatief **voorziet niet** in medefinanciering door derden.

3.3. Geraamde gevolgen voor de ontvangsten

– ☐ Het voorstel/initiatief heeft geen financiële gevolgen voor de ontvangsten

– ☒ Het voorstel/initiatief heeft de hieronder beschreven financiële gevolgen:

– ☐ voor de eigen middelen

– ☒ voor de diverse ontvangsten

miljoen EUR (tot op drie decimalen)

Begrotingsonderdeel voor ontvangsten:	Voor het lopende begrotingsjaar beschikbare kredieten	Gevolgen van het voorstel/initiatief[100]								
		Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**	Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**
Artikel 6313 - Bijdrage van de geassocieerde Schengenlanden (CH, NO, LI, IS)…… …….		p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.

Vermeld voor de diverse ontvangsten die worden "toegewezen" het betrokken begrotingsonderdeel of de betrokken begrotingsonderdelen voor uitgaven.

18.0207

Vermeld de wijze van berekening van de gevolgen voor de ontvangsten.

De begroting omvat een bijdrage van de landen die volgens de respectieve overeenkomsten betrokken zijn bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis en de Eurodac-maatregelen.

[100] Voor traditionele eigen middelen (douanerechten en suikerheffingen) moeten nettobedragen worden vermeld, d.w.z. na aftrek van 25 % aan inningskosten.